digitaleseniorInnen
Servicestelle für Bildungseinrichtungen

INTERNETKRIMINALITÄT

Leitfaden für Trainerinnen und Trainer

Informationen, Tipps und Materialien für den Unterricht

IMPRESSUM

Leitfaden für Trainerinnen und Trainer

Medieninhaber und Herausgeber:
Bundesministerium für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMSGPK)
Stubenring 1, 1010 Wien

Redaktion:
Österreichisches Institut für angewandte Telekommunikation
Ungargasse 64–66/3/404, 1030 Wien

Autorinnen: Edith Simöl, Valentine Auer, Thorsten Behrens, Declan Hiscox, Sandra Pöheim

Design: Confici · Kreativbüro, Franziskanerplatz 5/3/31, 1010 Wien

Erstellt im Auftrag des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz.

Bundesministerium
Soziales, Gesundheit, Pflege
und Konsumentenschutz

öiat

digitaleseniorInnen

LIEBE TRAINERIN, LIEBER TRAINER,

das Internet bietet viele Vorteile und kann den Alltag erleichtern. Die Welt der digitalen Medien ist gleichzeitig vielfältig und herausfordernd. Für die sichere Nutzung des Internets ist es wichtig über mögliche Gefahren Bescheid zu wissen. Die Aufgabe von EDV-Trainerinnen und EDV-Trainern ist, ältere Menschen über Betrugsfallen im Internet zu informieren, ohne Angst zu machen und auch das eigene Wissen auf dem aktuellen Stand zu halten.

Der vorliegende Leitfaden „Internetkriminalität“ informiert über gängige Betrugsfallen im Internet, zeigt, wie diese entlarvt werden können und unterstützt bei der Planung und Umsetzung von digitalen Unterrichtseinheiten für die Zielgruppe der Seniorinnen und Senioren.

Der Leitfaden gliedert sich in zwei Teile:

TEIL I: BEDROHUNGEN IM INTERNET

TEIL II: HANDBUCH ZUR UNTERRICHTSGESTALTUNG

Kontakt:
Servicestelle digitaleSeniorInnen
Ungargasse 64–66/3/404, 1030 Wien
Telefon: +43 1 595 21 12
E-Mail: office@digitaleSeniorInnen.at
Web: www.digitaleSeniorInnen.at

INHALT

TEIL I:

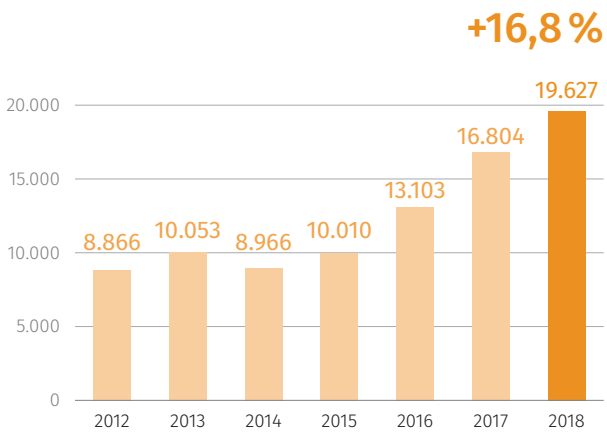
BEDROHUNGEN IM INTERNET

FAKTEN UND ZAHLEN

Durch die Digitalisierung entstehen neue Möglichkeiten der Kommunikation, der Zusammenarbeit und der Nutzung von neuen Online-Diensten, diese bringen uns viele Vorteile. Das Internet bietet jedoch zugleich Kriminellen ein attraktives Umfeld für ihre Taten.

Der Bereich der Internetkriminalität nimmt stetig zu. Opfer sind nicht nur Privatpersonen, sondern auch Unternehmen und Behören. Die Ausforschung von Täterinnen und Tätern wird erschwert, da diese kaum Datenspuren hinterlassen, es keine Tatorte und Zeuginnen und Zeugen gibt und die Angriffe über Ländergrenzen hinweg einfach durchzuführen sind.

„Die Kriminalität verlagert sich weiter zunehmend ins Internet."



Quelle: Bundeskriminalamt Österreich – Cybercrime 2018

Abb. 1: Internetbasierte Straftaten

Cybercrime im engeren Sinne umfasst kriminelle Handlungen, bei denen Angriffe auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik (IKT) begangen werden. Die Straftaten sind gegen die Netzwerke selbst oder aber gegen Geräte, Dienste oder Daten in diesen Netzwerken gerichtet (z. B. Datenbeschädigung, Hacking, DDoS-Angriffe).

Quelle: https://bundeskriminalamt.at/306/files/Cybercrime_Report_18_web.pdf

BETRUGSFALLEN ERKENNEN UND VERHINDERN

Die folgenden Beschreibungen von Betrugsfallen umfassen die Funktionsweise, Erkennungsmerkmale und mögliche Lösungswege für Opfer.

ABO-FALLEN IM INTERNET

Unter den am häufigsten auftretenden Betrugsmaschen im Internet finden sich betrügerische Abonnements – auch „Abo-Fallen" genannt. Darunter versteht man vermeintlich kostenlose oder günstige Dienste und Angebote, die später zu hohen Rechnungen oder automatisierten Abbuchungen führen. Als Lockmittel nützen Kriminelle beispielsweise Gewinnspiele, Streaming-Angebote oder Rezeptideen. Die Kosten werden später automatisiert abgebucht oder es werden einschüchternde Zahlungsaufforderungen, Mahnungen und Inkassoschreiben verschickt.

Abb. 2: Abo-Falle

Wie werden potenzielle Opfer in die Falle gelockt?

Um neue Opfer in Abo-Fallen zu locken, bewerben die Kriminellen ihre Dienste meist als kostenlos oder verlangen nur äußerst niedrige Summen. Es geht ihnen nämlich darum, möglichst viele Personen zu einer Eingabe ihrer persönlichen Daten oder gar zu einer Zahlung per Kreditkarte zu bringen. Sie setzen dabei auf angebliche Gewinnspiele, bieten kostenloses Streaming von Filmen und Serien nach einer einfachen Anmeldung an oder bewerben Rezeptideen und Routenplaner, bei denen die Angabe der E-Mail-Adresse notwendig ist, um die abgefragten Informationen zu erhalten. Für einen ersten Kontakt zu möglichen Opfern veröffentlichen sie Werbung für die betrügerischen Angebote auf Social-Media-Plattformen, erstellen Websites, auf der Ergebnisliste von Suchmaschinen, oder versenden massenhaft betrügerische E-Mails und SMS, die zu den Abo-Fallen führen.

Abo-Fallen mit automatisierten Abbuchungen

Bei Abo-Fallen, die zu automatisierten Abbuchungen führen, haben es die Kriminellen meist auf die Kreditkartendaten ihrer Opfer abgesehen. Um an diese zu gelangen, geben sie sich als bekanntes Unternehmen aus, das beispielsweise hunderte Smartphones, Wertgutscheine oder Tablets verlost, oder versenden Mails und SMS im Namen von Versanddiensten, in denen die Zahlung eines kleinen Betrages für den Erhalt eines Pakets verlangt wird. Dies läuft beispielsweise folgendermaßen ab:

- Das Opfer erhält eine E-Mail, die angeblich von Apple stammt.
- Das Unternehmen feiert angeblich Geburtstag und verschenkt deshalb 500 iPhones.
- Über einen Link gelangt das Opfer auf eine Website im Apple-Design.
- Hier wird nochmals erläutert, weshalb die iPhones verschenkt werden und womöglich sind auch Kommentare erfreuter Gewinnerinnen und Gewinner zu finden.
- Um selbst ein Gerät zu erhalten, soll das Opfer die eigenen Daten bekanntgeben.
- Im letzten Schritt ist die Zahlung eines Euros per Kreditkarte notwendig. Dies soll beispielsweise der Prüfung der Identität dienen oder die Versandkosten begleichen.

Das Opfer glaubt, in Kürze ein neues iPhone zu erhalten, tatsächlich kommt es aber zu laufenden Abbuchungen über die Kreditkarte. Das Gerät wird nie verschickt und die Abbuchungen von der Kreditkarte bleiben mitunter über Monate oder Jahre unentdeckt, wodurch teilweise hohe Schadenssummen zustande kommen.

Die folgenden Lockmittel werden häufig für diese Art des Betrugs gewählt:

- Kostenlose elektronische Geräte
- Kinogutscheine
- Einkaufsgutscheine
- Versand- oder Zollkosten
- IQ-Testergebnisse

Was kann gegen Abo-Fallen mit automatisierten Abbuchungen getan werden?

Unter keinen Umständen besteht ein gültiger Rechtsgrund für die automatisierten Abbuchungen, denn hierfür wären klare Angaben sämtlicher entstehenden Kosten, der Kündigungsbedingungen und der tatsächlich erbrachten Leistungen notwendig. Durch versteckte oder fehlende Kostenhinweise sind diese Bedingungen aber keinesfalls erfüllt. Sofern Kontaktinformationen zum Unternehmen zu finden sind, kann daher jeglichen Abbuchungen widersprochen und eine Rückbuchung gefordert werden.

Nicht immer ist eine Kontaktaufnahme möglich oder zielführend. Gemäß § 67 ZaDiG 2018 sind Beträge, die ohne Zustimmung des Opfers abgebucht wurden, vom Zahlungsdienstleister zurückzuerstatten. Das heißt, dass sich Opfer derartiger Betrugsmaschen an ihr Kreditkartenunternehmen wenden und eine Rückbuchung aller Abbuchungen fordern können, die über den tatsächlich freigegebenen Betrag hinausgehen. Liegen die Abbuchungen jedoch schon zu lange zurück, ist das Geld in aller Regel verloren, da auch das Kreditkartenunternehmen keine Handhabe mehr über die Geldbeträge hat.

Abo-Fallen mit personalisierten Zahlungsaufforderungen

Bei Abo-Fallen, die nicht zu automatisierten Abbuchungen führen, haben es die Kriminellen nicht auf die Zahlungsdaten ihrer Opfer abgesehen. Stattdessen reicht bereits eine E-Mail-Adresse für die Durchführung des Betruges aus. Um die E-Mail-Adressen und unter Umständen einige weitere Informationen über ihre Opfer zu erhalten, bieten die Kriminellen kostenlose Dienste an und verlangen dafür eine kurze Anmeldung per E-Mail-Adresse. Dies läuft beispielsweise folgendermaßen ab:

- Das Opfer googelt einen Film und möchte diesen kostenlos streamen.
- Es landet auf einer Website, die den Film im Angebot hat. Um den Film ansehen zu können, sei lediglich eine kostenlose Registrierung mit dem Namen und der E-Mail-Adresse notwendig.
- Das Opfer meldet sich wie beschrieben an, erhält aber keinen Zugriff auf den Film und über die nächsten Wochen gerät die Anmeldung in Vergessenheit.
- Plötzlich erhält das Opfer aggressive Zahlungsaufforderungen, weil eine angebliche Testphase abgelaufen und nun ein Premium-Abo zu bezahlen sei.
- Wird nicht bezahlt, folgen gefälschte Mahnungen, Inkasso-Schreiben und Pfändungs-Androhungen.
- Ruft das Opfer die Website, auf der die Anmeldung erfolgte, erneut auf, wird plötzlich klar auf Kosten hingewiesen, um für Verunsicherung zu sorgen.

Die Kriminellen versenden die Zahlungsaufforderungen automatisiert über Newsletter-Programme an alle Personen, die sich auf den Plattformen angemeldet haben. Sie erreichen dadurch eine große Menge an Menschen und hoffen dabei darauf, dass sich jemand von den Zahlungsaufforderungen einschüchtern und zu einer Zahlung bewegen lässt. Egal, ob bezahlt wird oder nicht – Filme können auf den Websites nie gestreamt werden und meist folgen trotz Zahlung weitere Zahlungsaufforderungen und Inkasso-Schreiben.

Die folgenden Lockmittel werden häufig für diese Art des Betrugs gewählt:

- Streaming-Angebote
- Routenplaner
- Koch- und Backrezepte
- Urlaubsbuchungs-Plattformen
- Dating- und Erotik-Portale mit Fake-Profilen

Was kann gegen Abo-Fallen mit personalisierten Zahlungsaufforderungen getan werden?

Wer ausschließlich Zahlungsaufforderungen erhalten, aber noch nicht bezahlt hat, kann einfach alle weiteren Nachrichten in dieser Sache ignorieren und muss nichts bezahlen. Es besteht kein gültiger Rechtsgrund für eine Zahlung der Forderungen. Die Nachrichten können gelöscht oder in den Spam-Ordner verschoben und die Absende-Adressen blockiert werden.

Sollte das Opfer bereits bezahlt haben, ist das Geld in aller Regel verloren, denn die Beträge werden per Banküberweisung gefordert und sind dadurch nur schwer bis gar nicht rückholbar. Sobald das Geld nämlich auf dem Zielkonto eingetroffen ist, muss die kontoführende Person bzw. deren Empfängerbank einer Rückbuchung zustimmen. Ein Zugriff auf Filme ist trotz Zahlung nicht möglich und es kann lediglich Anzeige erstattet werden.

Unrechtmäßige Abo-Verlängerungen

Wird der Begriff Abo-Falle breiter ausgelegt, fallen auch Dienste und Angebote darunter, bei denen kostenlose Probe-Phasen unter Missachtung gesetzlicher Vorgaben in kostenpflichtige Mitgliedschaften überlaufen. Eine derartige automatische Vertragsverlängerung ist nur dann gültig, wenn dies bei Vertragsabschluss bereits beispielsweise in den AGB vereinbart wurde, die Kundin oder der Kunde vor der automatischen Vertragsverlängerung einen Hinweis auf das Ende der Kündigungsmöglichkeit erhält und eine angemessene Frist für den Widerspruch gegen die automatische Verlängerung gegeben ist. Werden diese Bedingungen nicht erfüllt, ist die automatisierte Vertragsverlängerung ungültig.

Kündigungsschwierigkeiten

Zwielichtige Abonnement-Angebote versuchen außerdem häufig eine Kündigung zu erschweren. So kann es passieren, dass eine Kündigung laut AGB ausschließlich per Fax möglich sein soll oder gar keine Kontakt-Mail-Adresse vorhanden ist. Es ist daher ratsam, bereits vor einer Anmeldung auch genau auf die Kündigungsmodalitäten zu achten.

Weiterführende Links:

https://www.watchlist-internet.at/news/detail/News/so-schuetzen-sie-sich-vor-abo-fallen-im-internet/

https://www.watchlist-internet.at/news/detail/News/wenn-sie-in-eine-abo-falle-getappt-sind/

https://www.watchlist-internet.at/news/zahlungsaufforderungen-von-angeblichen-streamingdiensten-sind-fake/

https://www.watchlist-internet.at/news/gratis-iphone-11-oder-samsung-galaxy-s20-durch-hofer-umfrage/

ANLAGEBETRUG IM INTERNET

Der Anlagebetrug im Internet nimmt zu und stellt aufgrund teils enormer Schadensummen ein großes Problem dar. Den Opfern werden dabei schier unglaubliche Gewinnmöglichkeiten vorgespielt, die durch kleine Startinvestments – beispielsweise in Bitcoin oder andere Kryptowährungen – erreicht werden können. Werbung mit bekannten Gesichtern, persönliche Betreuung, ausgefeilte Nutzeroberflächen führen dazu, dass Betroffene mitunter mehrere hunderttausend Euro in betrügerische Trading-Plattformen investieren. Die Zahlungen landen auf ausländischen Konten und Auszahlungen angeblicher Gewinne sind nicht möglich. Das Geld ist somit verloren und Ermittlungen verlaufen meist im Sand.

Wie werden potenzielle Opfer angelockt?

Die Kriminellen hinter betrügerischen Investitionsplattformen setzen unterschiedliche Methoden ein, um potenzielle Opfer zu einer ersten Anmeldung und folglich einer Einzahlung zu bewegen:

- Sie verfassen erfundene Nachrichtenbeiträge und bewerben diese auf Social-Media-Plattformen.
- Sie missbrauchen die Gesichter prominenter Personen und behaupten, dass diese durch die jeweiligen Plattformen noch reicher geworden wären.
- Sie nützen die Logos bekannter Medien und Marken, um Vertrauen zu stiften.
- Sie erfinden Kommentare angeblicher Nutzerinnen und Nutzer, die mit kleinen Einzahlungen hohe Gewinne erzielen konnten.
- Sie versenden E-Mails, nehmen Kontakt über Dating-Plattformen oder Spiele-Chats auf und versuchen im persönlichen Kontakt zu ersten Einzahlungen zu bewegen.

Wie werden Opfer zu hohen Einzahlungen bewegt?

Nach der ersten Anmeldung bei einer betrügerischen Investitionsplattform folgt in aller Regel ein Anruf der persönlichen Betreuerin oder des persönlichen Betreuers. Dies soll Vertrauen stiften, gleichzeitig wird das weitere Vorgehen erläutert. Die ersten Einzahlungen bewegen sich meistens zwischen 200 und 300 Euro. Über die ausgefeilten Websites werden daraufhin in kürzester Zeit die angeblichen Gewinne dargestellt. Aufkommende Euphorie wird von den Kriminellen dann ausgenützt, um zu weiteren Zahlungen zu bewegen. Dabei gilt: Je höher die Einzahlung, desto höher fällt der angebliche Gewinn aus. Wer sich beispielsweise entscheidet, 10.000 statt 1.000 Euro einzuzahlen, erhält bessere Konditionen und wird zukünftig von erfolgreicheren Traderinnen und Tradern betreut.

Dieses Spiel setzt sich so lange fort, bis die Opfer kein Geld mehr einzahlen. Stellen die Kriminellen fest, dass die Zahlungsmotivation sinkt, stellen sie ihre Taktik um: Plötzlich kommt es zu hohen Verlusten. Um diese zu kompensieren, sollen sofort weitere Einzahlungen erfolgen, die für Investitionen in andere Märkte genützt werden. Später werden Fehler der bisherigen persönlichen Betreuung als Begründung für (Total-)Verluste genannt. Die Person sei deshalb sofort gekündigt worden. Durch weitere Investitionen mit einer neuen persönlichen Betreuerin oder einem neuen persönlichen Betreuer könnten sämtliche Verluste schnell wieder behoben werden.

Ein Fallbeispiel, welches sich so zugetragen hat, zeigt auf, wie dieses Vorgehen zu horrenden Schadensummen führt:

- Einzahlung nach Anmeldung: 250 Euro
- Einzahlung für höhe Gewinnchancen: 1.000 Euro
- Einzahlung für erfahrenere Betreuung: 4.000 Euro
- Einzahlung für Investition in andere Märkte: 15.000 Euro

Binnen weniger Wochen wurden 20.000 Euro investiert. Nachdem zwischenzeitlich unglaubliche „Gewinne“ erzielt werden konnten, was den dargestellten Kontostand in den sechsstelligen Bereich steigen ließ, werden nun plötzlich erste Verluste eingefahren. Um diese aufzuhalten, wird zu weiteren Einzahlungen aufgefordert.

→ Einzahlung für Investition in andere Märkte zur Kompensation der Verluste: 30.000 Euro

Nachdem wieder Gewinne eingefahren werden konnten, verlangte das Opfer eine sofortige Auszahlung des Gesamtkapitals, doch es folgte ein plötzlicher Verlust des Gesamtkapitals binnen kürzester Zeit, noch bevor die Auszahlung erfolgen konnte. Die Verzweiflung über den Verlust sämtlicher Gewinne und der investierten 50.000 Euro wurde ausgenützt, um das Opfer zu einer neuerlichen Einzahlung zu bewegen. Die Verluste sollten mithilfe des besten Traders im Unternehmen wieder wettgemacht werden.

→ Einzahlung zur Kompensation der Verluste: 50.000 Euro

Insgesamt bezahlte das Opfer in diesem Fall über 100.000 Euro an die Kriminellen, ehe der betrügerische Hintergrund endgültig aufflog und keine weiteren Einzahlungen mehr erfolgten.

Die Kriminellen setzen häufig weitere Methoden ein, um den Opfern das Geld aus der Tasche zu ziehen:

- Sie setzen auf Zeitdruck und verlangen Zahlungen sofort, um Gewinnchancen nicht zu verpassen.
- Beharrt ein Opfer auf einer Auszahlung, so werden vorab zu bezahlende Gebühren, Steuern oder Anteile verlangt.
- Die Opfer werden zur Kreditaufnahme gedrängt, um weitere Investitionen tätigen zu können, falls kein Budget mehr vorhanden ist.
- Ist das Gesamtkapital bereits verloren und der Kontakt zur Trading-Plattform abgebrochen, werden die Opfer zu vermeintlichen Rückholdiensten weitergeleitet oder gezielt von diesen kontaktiert. Diese behaupten die Einzahlungen gegen Vorabzahlung zurückholen zu können. Die Dienste stammen aber von den Kriminellen selbst und erhöhen lediglich den Gesamtverlust.

Zugriff per Fernwartungssoftware AnyDesk

Viele der betrügerischen Plattformen setzen nicht nur auf die telefonische Betreuung ihrer Opfer, sondern verlangen Zugriff auf deren Computersystem über die Fernwartungssoftware AnyDesk. Sie behaupten, ihre Klientinnen und Klienten so besser betreuen zu können. Durch die Software wird es den Kriminellen ermöglicht, aus der Ferne das System ihrer Opfer zu steuern. In Verbindung mit dem Onlinebanking-Zugang können sie so selbst Einzahlungen tätigen. Auch die Installation von Schadsoftware, die beispielsweise sensible Daten und Passwörter ausliest, ist dadurch möglich. Weitere Schäden sind somit nicht auszuschließen.

Wie bleiben die Kriminellen unentdeckt?

Die Betrügerinnen und Betrüger setzen alles daran, ihre Identitäten geheim zu halten. Sie wenden daher unterschiedliche Tricks an, um unentdeckt zu bleiben:

- Sie registrieren ihre Unternehmen auf „Offshore-Inseln“ – darunter versteht man Jurisdiktionen, die keine oder kaum Überprüfungen von Finanztransaktionen durchführen, kaum Steuern einheben und nur minimale Vorgaben zur Unternehmenseröffnung

vorschreiben. Bekannte Beispiele sind die Cayman Inseln oder Panama.
- Sie setzen Anonymisierungsdienste ein, sodass beispielsweise nicht nachvollziehbar ist, wer die Website oder das Unternehmen registriert hat.
- Sie betreiben Geldwäsche, um die Rückverfolgung von eingezahlten Geldern zu erschweren oder unmöglich zu machen.

Wie kann man sich vor derartigen Betrugsmaschen schützen?

Für den Schutz vor Investmentbetrug ist insbesondere ein gewisses Maß an Medienkompetenz und Skepsis den unglaublichen Versprechungen gegenüber gefragt. Dadurch sind beispielsweise die Werbeschaltungen auf Social-Media-Plattformen oder die gefälschten Nachrichtenartikel leicht als betrügerisch erkennbar. Konkrete Tipps zur frühzeitigen Erkennung unseriöser Investitionsmöglichkeiten sind beispielsweise folgende:

- Wird mit unglaublich hohen Renditen bei kleinem Investment ohne jegliche Vorkenntnisse geworben, ist Abstand zu nehmen.
- Besitzt die Website ein Impressum und hat die Firma einen Sitz in der EU oder einem anderen Staat mit strengen Finanzmarktregulierungen? Wenn nicht, sollte niemals Geld investiert werden.
- Es sollte nach Erfahrungsberichten zu den Plattformen gesucht werden. Oft lässt sich schnell feststellen, dass es sich um Betrug handelt, da bereits zahlreiche Warnungen veröffentlicht wurden. Auch wenn weder negative noch positive Berichte vorhanden sind, ist Vorsicht geboten. Es könnte sich um ein neues Betrugsangebot handeln.
- Die Finanzmarktaufsicht (FMA) veröffentlicht laufend aktuelle Investorenwarnungen unter https://www.fma.gv.at/category/news/?cat=42&filter-dropdown-year=&filter-dropdown-order=date_desc. Diese können vor Investments durchsucht werden.
- Wird die Installation von Fernwartungssoftware wie AnyDesk verlangt, um Investments durchzuführen, handelt es sich um Betrug. Jeglicher Kontakt muss sofort abgebrochen werden.

Wurde bereits Geld auf einer betrügerischen Plattform investiert, so fällt es Betroffenen erfahrungsgemäß äußerst schwer, zu akzeptieren, dass sie Opfer eines Betrugs wurden und weitere Investitionen den Schaden nur vergrößern würden. Die Akzeptanz der Tatsachen ist daher äußerst wichtig, um weitere Verluste zu vermeiden und den Kontakt zu den Kriminellen abbrechen zu können. In aller Regel bleibt ausschließlich der Gang zur Polizei, die Meldung an die FMA und eine Anfrage bei der Bank, ob Teilbeträge unter Umständen noch rückholbar sind.

Weiterführende Links:

https://www.watchlist-internet.at/news/online-anlagen-und-investitionsbetrug-floriert/

https://www.watchlist-internet.at/news/detail/News/investment-firmen-fordern-zugriff-auf-ihr-system-nehmen-sie-abstand/

https://www.watchlist-internet.at/news/detail/News/kriminelle-nuetzen-promis-und-medien-fuer-bitcoin-betrug/

BETRUG & WERBUNG

Ob auf Google, in sozialen Medien oder in Apps – überall lauert Werbung, die uns dazu bringen will, ein bestimmtes Produkt zu kaufen oder eine Dienstleistung in Anspruch zu nehmen. Doch nicht jede Werbung ist seriös. Unter den vielen legitimen Werbetreibenden finden sich auch immer wieder Kriminelle.

Soziale Medien

In den sozialen Medien sind wir von Werbung umgeben. Insbesondere Facebook und Instagram gelten als lukrative Werbekanäle. Das ist für viele Nutzerinnen und Nutzer nicht nur nervig, sondern manchmal sogar gefährlich, denn auch Kriminelle nutzen zunehmend Werbung in den sozialen Medien, um auf sich aufmerksam zu machen.

> **Gut zu wissen:** Auf Facebook und Instagram können Unternehmen (aber auch Vereine oder andere Organisationen) dafür bezahlen, dass ein bestimmter Beitrag nicht nur jenen Menschen, die der werbenden Seite folgen oder diese liken, angezeigt wird, sondern auch vielen anderen. Dafür kann eine bestimmte Zielgruppe festgelegt werden. Auf Facebook werden Werbeanzeigen entweder am rechten Rand (bei der Desktop-Version) oder direkt im Feed als „gesponsert" angezeigt – also zwischen den Beiträgen, die man durchscrollt. Auch für Instagram gibt es diese Möglichkeit, hier können die Werbeanzeigen im Feed oder zwischen verschiedenen Instagram-Storys angezeigt werden. Da Instagram zu Facebook gehört, kann ein erstellter Werbebeitrag für beide Kanäle genutzt werden.

Immer öfter berichten Opfer von Fake- oder Markenfälscher-Shops, dass sie über eine Facebook- oder Instagram-Werbung auf einen betrügerischen Onlineshop gestoßen sind. Vor allem unseriöse Modeshops gibt es viele in den sozialen Netzwerken. Über gesponserte Bei-

träge versuchen diese an ihre Opfer zu kommen, indem sie besondere Angebote bewerben.

Abb. 3: Modeshop-Facebook-Werbung

BEISPIEL MODESHOPS:

Während der Coronakrise tauchten viele Modeshops auf, welche die Krise angeblich nicht überstanden haben und nun günstig Kleidung verkaufen. Dies las sich in den Feeds oder auch zwischen den Storys folgendermaßen: „Es tut uns leid, dass unser Bekleidungsgeschäft diese Katastrophe nicht überlebt hat. Wir haben beschlossen, den größten Teil der restlichen Kleidung zu einem niedrigeren Preis zu verkaufen." Oder: „Aufgrund der jüngsten besonderen Situation müssen wir die Kollektion schließen und daher den Lagerbestand zu einem niedrigsten (sic) Preis verkaufen. Ausverkauf!! Die letzten Tage!!! Überraschend günstig, WoW Preise (sic)."

Doch nicht nur betrügerische Modeshops sind auf Facebook und Instagram beliebt. Fake-Shops bewerben verschiedene Produkte in den sozialen Medien. Auch Bitcoin-Betrug, Abo-Fallen und Phishing finden immer wieder durch Werbeanzeigen in sozialen Medien Verbreitung.

Wie gehen Facebook und Instagram gegen betrügerische Werbung vor?

Die Werberichtlinien von Facebook und damit auch von Instagram verbieten Werbung für irreführende Produkte und Dienstleistungen. Dafür werden Algorithmen verwendet, mit denen jede Anzeige automatisch überprüft wird.

Allerdings finden die Kriminellen immer neue Wege, um die automatische Überprüfung zu umgehen. Sehr beliebt ist das sogenannte Cloaking: Bei der automatischen Überprüfung der Anzeige ist für Facebook nur ein harmloser Link sichtbar. Tatsächlich ist die Seite, auf die man beim Anklicken der Werbung gelangt, eine andere, betrügerische Seite. Die betrügerische Absicht der Werbung wird so verschleiert.

Konnten die Kriminellen die Anzeige veröffentlichen, gibt es aber auch im Nachhinein die Möglichkeit dagegen vorzugehen, indem einzelne Nutzerinnen und Nutzer betrügerische Werbeanzeigen melden. Sobald Facebook oder Instagram Kenntnis von solchen Anzeigen erhält, werden diese gelöscht und die dazugehörige Seite gesperrt. Die Erfahrung zeigt jedoch, dass diese von Menschen durchgeführte Überprüfung aufgrund der Masse an betrügerischen Anzeigen sehr lange dauern kann. Bis es zu einer Löschung kommt, gibt es oftmals bereits viele Opfer.

So wird eine Anzeige als betrügerisch gemeldet: Sowohl auf Facebook als auch auf Instagram gibt es neben jedem Beitrag drei Punkte, die angeklickt werden können. Es öffnet sich ein Menü, dort findet sich der Punkt „Werbeanzeige melden".

Wie können betrügerische Werbeanzeigen auf Facebook und Instagram entlarvt werden?

Das dazugehörige Profil kann Aufschluss darüber geben, ob es sich um ein seriöses Angebot handelt. Hinweise darauf können folgende Punkte sein:

- Seiten mit betrügerischer Absicht werden von den Nutzerinnen/Nutzern immer wieder als betrügerisch gemeldet und von Facebook und Instagram gesperrt. Daher sind betrügerische Seiten oftmals noch recht neu. Auf jeder Facebook-Seite finden Sie den Punkt „Seitentransparenz", der Aufschluss darüber gibt, wann die Seite erstellt wurde.
- Nur wenige Likes und Beiträge sind für einen Onlineshop ungewöhnlich. Daher kann auch dies auf Betrug hinweisen.
- Unter den Beiträgen der betrügerischen Seite finden sich oftmals Kommentare, die von negativen Erfahrungen berichten.

Google

Wird bei der Google-Suche eine Seite ganz oben in der Liste der Suchergebnisse angezeigt, wird diese auch öfters angeklickt. Das ist der Grund, wieso Kriminelle Google-Anzeigen nutzen, um möglichst viele Opfer anzusprechen.

Wie in den sozialen Netzwerken gibt es auch bei Google Werberichtlinien, an die sich alle Werbetreibenden halten müssen. Dass diese Richtlinien oft verletzt werden, zeigt jedoch der jährliche „Trust & Safety in Ads Report" von Google. Laut diesem hat Google 2019 2,7 Milliarden unangemessene Anzeigen entfernt. Das entspricht 5.000 Anzeigen pro Minute. Besonders vertraut ist Google dabei mit Phishing-Anzeigen. Ganze 35 Millionen solcher Anzeigen wurden 2019 entfernt.

Beispiel Reisepass-Verlängerung: Es sind vermehrt Betrügerinnen und Betrüger aufgefallen, die mithilfe einer Google-Werbeanzeige günstige Reisepass-Verlängerungen bewerben. Die Links in diesen Anzeigen führen zu Websites, die seriösen Angeboten stark ähnelten. Die Absicht dahinter: Die Opfer sollen sensible Informationen wie Sozialversicherungs- oder Kreditkartennummern eingeben. Diese landen dann direkt in den Händen der Kriminellen.

Beliebt sind auch sogenannte „Trick-to-Click"-Anzeigen. 2019 wurden 19 Millionen solcher Anzeigen blockiert. Sie sollen zum Anklicken eines bestimmten Links verleiten, der auf eine betrügerische oder unseriöse Website führt. Deshalb verwenden die Kriminellen auffällige Anzeigen, die für die Nutzerinnen und Nutzer beispielsweise wie ein Warnhinweis oder ein Gewinnspiel aussehen.

Natürlich zahlen auch Betreiberinnen oder Betreiber von Fakeshops viel Geld an Google, um sichtbar zu sein. Wird nach einem bestimmten Produkt gesucht, werden Fakeshops, die angeben diese Produkte zu verkaufen, als Anzeige ganz oben in der Suchergebnisliste angezeigt.

Trust & Safety in Ads Report: https://blog.google/products/ads/stopping-bad-ads-to-protect-users/

Beispiel für unseriöse Notdienste

Gleiches gilt auch für Dienstleistungen. Oftmals nutzen Betrügerinnen und Betrüger Notsituationen aus, in denen es schnell gehen muss. Bei einem Stromausfall, einem Wasserrohrbruch oder einem Gasgebrechen muss rasch eine Expertin oder ein Experte her. Für die Überprüfung eines Installations- oder Elektrik-Notdienstes bleibt da häufig keine Zeit mehr. Das nutzen unseriöse Handwerksbetriebe aus. Mithilfe von bezahlten Anzeigen schaffen es diese, bei bestimmten Suchbegriffen (zum Beispiel „Installateur Wien" oder „Elektriker Tirol") ganz oben in der Liste aufzuscheinen.

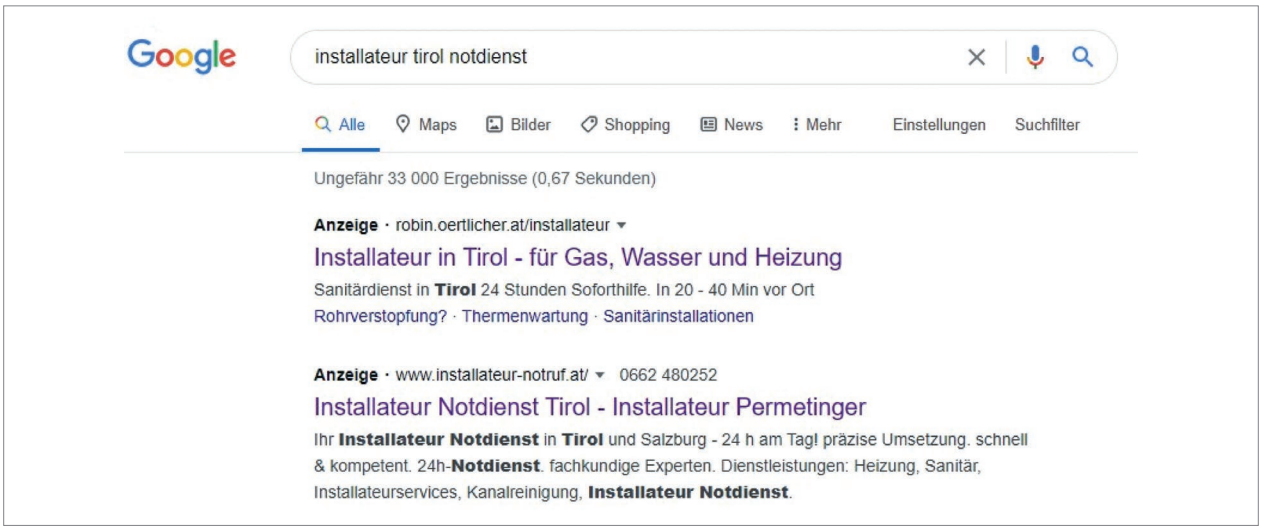


Abb. 4: Fake-Notdienste auf Google

Sieht man sich die Websites der vermeintlichen Handwerksbetriebe an, wird dort versprochen, jederzeit erreichbar zu sein und dass Profis innerhalb von 45 Minuten vor Ort sein könnten. Dies ist genau das, was Menschen in dieser Notsituation brauchen. Rufen die Opfer an, um Hilfe anzufordern, kommen die Handwerkerinnen und Handwerker auch tatsächlich und kümmern sich um die Schäden (oder geben vor, sich dar-

um zu kümmern). Das Problem dabei: Im Nachhinein werden überhöhte Kosten in Rechnung gestellt, die bar bezahlt werden müssen und von vielen in der Notsituation akzeptiert werden. Da die Handwerksbetriebe keine Gewerbeberechtigung vorweisen können und auf den Websites selten ein vollständiges Impressum zu finden ist, sind die Kriminellen bei Beschwerden nicht mehr erreichbar. Das Geld ist damit meist verloren.

So kann man sich vor unseriösen Notdiensten schützen:

- Den Google-Ergebnissen darf nicht blind vertraut werden. Auch in einem Notfall sollte man sich Zeit nehmen, um nach einem Impressum auf der Website zu suchen. Nur wenn man weiß, wer hinter dem Notdienst steckt, sollte dieser auch beauftragt werden.
- Seriöse Unternehmen geben außerdem die Zahlungsmöglichkeiten auf ihren Websites an. Fehlt diese Information, sollte man vorsichtig sein.
- Damit man in einer Stresssituation nicht auf unbekannte Anbieterinnen und Anbieter vertrauen muss, empfiehlt es sich eine Telefonliste mit vertrauenswürdigen Notfalldiensten aller Art anzulegen.

Wie kann man sich vor betrügerischen Werbeanzeigen auf Google schützen?

Google selbst arbeitet ständig an technischen Lösungen, um es Betrügerinnen und Betrügern schwerer zu machen. Gleichzeitig kritisieren Nichtregierungsorganisationen (NGOs) immer wieder, dass es für Kriminelle ein Leichtes ist, betrügerische Werbeanzeigen zu erstellen. Die britische NGO „Which?“ wollte beispielsweise wissen, wie leicht Fake-Unternehmen Anzeigen erstellen können. Dafür hat sie zwei unechte Unternehmen erfunden. Ein Unternehmen verkauft ein Produkt, das angeblich beim Gewichtsverlust unterstützt und die Stimmung verbessern soll. Das andere Unternehmen ist eine Fake-Plattform, die falsche Gesundheitstipps gibt. Um Werbeanzeigen für diese Unternehmen zu erstellen, war lediglich ein Profil bei Gmail notwendig. Die Anzeigen wurden zwar überprüft, allerdings recherchierte Google nicht, ob die Unternehmen tatsächlich existieren. Innerhalb einer Stunde wurden die Anzeigen genehmigt.

Dieses Experiment zeigt eindrücklich, dass das Überprüfungsverfahren von Google nicht ausreicht, um gegen betrügerische Werbung vorzugehen. Umso wichtiger ist es, dass Nutzerinnen und Nutzer unseriöse Werbeanzeigen erkennen und sich vor möglichen Betrugsmaschen schützen können. Folgende Punkte sind dabei wichtig:

- Schon die Anzeige kann manchmal Hinweise darauf geben, ob das dahinterstehende Unternehmen seriös ist: Gibt es viele Rechtschreib- oder Grammatikfehler in der Anzeige? Sind die verwendeten Bilder von schlechter Qualität? Ein seriöses Unternehmen, das viel Geld an Google bezahlt, wird auch darauf achten, dass die Anzeige ansprechend ist.
- Was wird in der Anzeige versprochen? Wie realistisch ist dieses Versprechen? Es ist wohl eher unrealistisch, dass unheilbare Krankheiten mit einem einzigen Produkt plötzlich geheilt werden können oder dass eine Person unzählige Menschen in nur wenigen Wochen zu Millionärinnen und Millionären macht.
- Auch wenn die Anzeige seriös wirkt, sollte das Unternehmen überprüft werden: Gibt es das Unternehmen wirklich? Welche Informationen lassen sich über das Unternehmen finden? Sind diese Informationen vertrauenswürdig?
- Um spätestens beim Klicken auf eine betrügerische Anzeige gewarnt zu werden, erkennen Browser (zum Beispiel Firefox, Chrome oder Safari) bereits manche Websites, die gefährlich sind. In den Sicherheitseinstellungen (meist mit einem Klick auf die drei Punkte oder Striche ganz rechts zu finden) können Schutzmaßnahmen wie das Blockieren von gefährlichen und betrügerischen Inhalten eingeschaltet werden.
- Zusätzliches Werkzeug kann helfen, sicher im Internet unterwegs zu sein: Zum Beispiel durch das „Netcraft Anti-Phishing“-Plugin, das vor gefälschten Websites warnt, oder „Trustnav Safesearch“, das Suchergebnisse, Websites und Werbeanzeigen überprüft.

Im Webbrowser vor Phishing-Attacken schützen: https://www.watchlist-internet.at/news/detail/News/im-webbrowser-vor-phishing-attacken-schuetzen/

Weitere betrügerische Werbeanzeigen

Google, Facebook und Instagram sind nicht die einzigen Plattformen, auf denen mit betrügerischer Werbung möglichst viele Menschen angesprochen werden. Werbeanzeigen für Fake-Shops finden sich beispielsweise auch auf seriösen Websites als Werbebanner. Verschiedene Arten von Anzeigen werden auch per E-Mail als Spam verschickt. Die Bandbreite solcher Mails reicht dabei von Werbung für betrügerische Trading-Plattformen über den Versuch per Werbung Schadsoftware auf dem Computer zu installieren bis hin zu fragwürdigen Produkten. Auch in verschiedenen Apps wie Handy-Spielen schleicht sich oftmals unseriöse Werbung ein. Daher gilt: Online-Anzeigen sollte man niemals blind vertrauen. Eine Überprüfung der dahinterstehenden Unternehmen und ein kritisches Hinterfragen der jeweiligen Versprechen helfen dabei, unseriöse Werbeanzeigen zu entlarven.

Weiterführende Links:

https://www.watchlist-internet.at/news/achtung-vor-betruegerischen-werbeanzeigen-auf-facebook-instagram-und-google/

https://www.watchlist-internet.at/news/unserioese-angebote-werben-mit-orf-promis/

https://www.watchlist-internet.at/news/zahlreiche-unserioese-china-shops-werben-auf-facebook-mit-guenstiger-damenmode/

https://www.watchlist-internet.at/news/detail/News/werbung-fuer-betruegerische-elektriker-auf-google/

IDENTITÄTSDIEBSTAHL

Bei vielen Geschäften im Internet werden Ausweiskopien verlangt – zum Beispiel bei der Wohnungssuche, bei der Eröffnung eines Kontos bei einer Onlinebank oder beim Abschluss eines Mobilfunkvertrags. Dies machen sich Kriminelle zu Nutze, denn Ausweiskopien und fremde Identitäten sind im Bereich der Internetkriminalität ein begehrtes Gut. Cyberkriminelle können so vorgeben eine andere Person zu sein und unter falschem Namen verschiedene Straftaten begehen.

Betrügerische Marktforschungsinstitute

Es gibt unterschiedliche Tricks, wie Kriminelle an fremde Identitäten gelangen. Eine beliebte Masche ist der Weg über Marktforschungsinstitute bzw. über Umfrageplattformen, die mithilfe von Stellenausschreibungen nach ihren Opfern suchen. Versprochen wird ein einfacher und unkomplizierter Nebenverdienst durch das Beantworten von Umfragen oder das Testen von Apps. Doch anstatt Geld zu auszuzahlen, wird im Namen der Opfer ein Bankkonto eröffnet. Die Vermutung liegt nahe, dass mit diesen Bankkonten Geldwäsche betrieben wird.

BEISPIEL PROANALYSES.DE

Die Website proanalyses.de ist ein Beispiel für eine solche Umfrageplattform. Bei der Anmeldung mussten die Interessentinnen und Interessenten ihre Ausweisdokumente hochladen. Im Rahmen der ersten angeblichen Umfrage sollten die Teilnehmenden ein Konto bei der Onlinebank „N26“ testen. Dafür ist die Durchführung eines Video-Ident-Verfahrens notwendig. Diese Verfahren werden verwendet, um sich per Videochat online zu identifizieren. Dafür muss den Anweisungen des Gegenübers gefolgt und auch ein Ausweis in die Kamera gehalten werden.

Im folgenden Text wird den Teilnehmenden erklärt, wie diese vermeintliche Umfrage durchzuführen ist:

Registration

Ihre Test-Zugangsdaten:

Bitte Zugangsdaten im Chat anfordern.
WICHTIG: Benutzen Sie die folgenden Logindaten, damit wir das Konto als DEMO zuweisen können!

Melden Sie sich mit den vorgegebenen Daten in der N26 App und geben Sie beim VideoIdent-Verfahren Ihre Daten gewissenhaft und ehrlich an. Bitte benutzen Sie die vorgegebenen Login-Daten, damit wir das Konto als DEMO werten können.

Was Sie beachten müssen:
Die N26 Bank will das Identifikationsverfahren, welches aktuell extern abgewickelt wird genau unter die Lupe nehmen. Die Mitarbeiter werden natürlich am besten überprüft, wenn Sie mit einem echten Kunden zu tun haben. Verhalten Sie sich also ganz natürlich, als würden Sie ein echtes Bankkonto eröffnen. Das Konto wurde bei der N26 als Demo erstellt und wird nach Überprüfung Ihres Berichts unwiderruflich gelöscht. Ihnen entstehen dabei keine Kosten.

Registrierung

Es geht unter anderem auch darum, das Angebot der N26 sowie die Funktion der App/den Registrierungsprozess zu testen und zu bewerten. Ihnen fallen natürlich keine Kosten an, da es sich um ein Demo-Konto handelt. Füllen Sie alle Daten gewissenhaft aus.

Bitte notieren Sie sich, ob die Mitarbeiter auf Betrug andeuten. Wir wurden beauftragt, um zu überprüfen, ob jeder Mitarbeiter darauf hindeutet. Sollte der Mitarbeiter darauf andeuten, dann sagen Sie, dass das Konto für Sie für das private Nutzen dient.

Bitte denken Sie daran, das Konto nach der Legitimierung nicht mit Ihrem Smartphone zu koppeln und auch kein Überweisungs-PIN zu setzen. Ansonsten können wir das Konto nicht als DEMO werten/löschen und den Auftrag nicht ausbezahlen.

Hier finden Sie mögliche Fragen des Mitarbeiters und eine angebrachte Antwort.

Haben Sie das Konto selbst erstellt?
Ja, das habe ich.

Wofür machen Sie diese Identifikation?
* Hier nennen Sie den Auftragsnamen, in diesem Fall N26. Nichts von einem Test erwähnen.

Bekommen Sie Geld für diese Identifikation/Test/Auftrag?

Nein, ich mache das privat.

Haben Sie Zugriff auf Ihre E-Mail?
Ja, das habe ich.

Machen Sie das für einen Job?
Nein, ich mache das privat.

Der Bericht

Halten Sie in Ihrem Bericht folgende Dinge fest:
- Ihren Namen und E-Mail
- Die Dauer der Registrierung
- Die Wartezeit
- Die Fragen, die sie vom Mitarbeiter gestellt bekommen
- Jegliche Details und verbesserungswürdige Punkte, aus Ihrer Sicht

WICHTIG: Führen Sie keine weiteren Schritte außer dem Verifikations-Test durch, damit keine weiteren Kosten entstehen!

Den Opfern werden also Zugangsdaten geschickt, mit denen sie sich in der N26-App anmelden können und anschließend das Video-Ident-Verfahren IDNOW durchführen sollen. Um den Mitarbeiterinnen und Mitarbeitern hinter dem IDNOW-Verfahren zu verheimlichen, dass das Opfer gar kein echtes Konto eröffnen möchte, werden genaue Vorgaben gemacht, wie auf bestimmte Fragen geantwortet werden soll und wie sich die Testerinnen und Tester zu verhalten haben – nämlich so, als würden sie ein echtes Konto eröffnen. Um die Opfer im Glauben zu lassen, tatsächlich lediglich eine Überprüfung des IDNOW-Verfahrens durchgeführt zu haben, wird außerdem ein Bericht verlangt, der nach dem Test erstellt werden soll. Zu einer Auswertung dieses Berichts oder einer Bezahlung für die Umfrage kommt es nicht. Stattdessen werden mit den gestohlenen Ausweiskopien und den eröffneten Bankkonten Verbrechen unter den Namen der Opfer begangen.

Gut zu wissen: Die Webseite proanalyses.de ist mittlerweile nicht mehr aktiv. Allerdings tauchen immer wieder neue Varianten dieser Portale auf. Die Watchlist Internet stellt eine Liste mit betrügerischen Umfrageplattformen zur Verfügung, um laufend davor zu warnen: https://www.watchlist-internet.at/liste-umfrageplattformen/

Betrügerische Stellenausschreibungen

Doch nicht nur Stellenausschreibungen für die Teilnahme an Umfragen oder für das Testen von Apps können zum Identitätsdiebstahl führen. Egal, ob man sich als Kinderbetreuerin oder Kinderbetreuer bewirbt oder auf einem Weihnachtsmarkt mitarbeiten will: Verlangen die vermeintlichen Arbeitgeberinnen oder Arbeitgeber einen Ausweis bei der Bewerbung, ist Vorsicht geboten.

BEISPIEL WEIHNACHTSMARKT

In Tageszeitungen und auf Kleinanzeigenplattformen inserierten Kriminelle eine Stelle für den Verkauf von Christbaumschmuck und Weihnachtsaccessoires. Interessierte Personen sollten im Rahmen ihrer Bewerbung eine Reisepasskopie an das Jobcenter Austria übermitteln.

***** *Mitarbeiter gesucht!* *****

Wir suchen ab sofort wieder österreichweit engagierte Damen und Herren, die uns in der vorweihnachtlichen Zeit unterstützen und uns behilflich sind im Verkauf von Christbaumschmuck und Weihnachtsaccessoires.

Arbeitszeit: 20 Stunden Woche (Freitag/Samstag)
Arbeitsbeginn: 1. bis 23. Dezember 2017
Verdienst: € 950,–/netto

Unsere 350 Verkaufsstände sind in Form von 3×3 Meter großen Holzhütten mit Beleuchtung und Deko fix und fertig für Sie bereits in diversen Shoppingcentern in ganz Österreich aufgestellt.

Für diese Tätigkeit sind keine besonderen Berufserfahrungen notwendig; ein fließendes Deutsch in Wort und Schrift sowie die Volljährigkeit werden jedoch vorausgesetzt.

Haben wir Ihr Interesse geweckt?

Dann senden Sie Ihre vollständigen Bewerbungsunterlagen inklusive einer Kopie (Foto) des Reisepasses an Hr. Ivanovic unter jobcenter.austria@outlook.com

Abb. 5: Fake-Stellenausschreibung

Meldeten sich Interessentinnen und Interessenten beim Jobcenter Austria und schickten die gewünschten Unterlagen mit, erfuhren diese rasch, dass sie an Kriminelle geraten sind. Als Rückmeldung erhielten die Opfer folgende E-Mail:

Herzlichen Dank für Ihre Bewerbung

Um es kurz zu machen es gibt keine freie Stelle zu vergeben. Diese Arbeitsstelle hat es auch nie gegeben. Jedoch vielen Dank für Ihre persönlichen Daten und Dokumente.
Diese Dokumente werde ich jetzt im Dark Web Online stellen und somit am Schwarzmarkt an den Höchstbietenden verkaufen.

Mit diesen Dokumenten kann man viel Scheiße bauen, ich sag nur Identitätsdiebstahl!!!
Dank Ihrer Persönlichen Unterlagen und Daten ist das nun ganz leicht machbar. Und dann haben Sie Probleme am Hals mit Inkasso Service, Anwälten, Kredithaien, Polizei usw.

Wenn Sie jetzt der Meinung sind Sie müssen zur Polizei laufen, weil die Ihnen helfen kann, FEHLANZEIGE!!!

Die können Ihnen definitiv nicht helfen da ich einen Server im Ausland benutze der nicht logt, das Internet via Wertkarte beziehe und meine Identität, welche Sie vermuten zu Wissen von Anfang an Falsch war.

Finden werden die mich definitiv nicht!!!

Also bezahlen Sie lieber den von mir genannten Betrag in Höhe von 300 € und folgen meiner Anweisung genauestens, danach werde ich sämtliche Dateien und Dokumente von Ihnen löschen und

Sie hören nie mehr wieder etwas von mir.

Wenn Sie mir das Geld übermittelt habe gebe ich Ihnen wieder Ihre Ruhe zurück!!!

1. Gehen Sie in eine/n Trafik, Tankstelle, Libro, Post, Spar, Merkur, Billa etc.
2. Kaufen Sie für 300 € Amazon Gutscheinkarten.
3. Sie bekommen dann sechs Bons zu à 50.
4. Danach machen Sie ein Bild von den Codes und leiten es mir via E-Mail weiter.
5. Nachdem ich die Bons geprüft habe werde ich es Ihnen mitteilen, dass Sie die Amazon Karten wegwerfen können.
6. Von diesem Moment an sind Ihre Dokumente gelöscht und Sie haben wieder Ihre Ruhe.

Eines sollten Sie noch Wissen, das ist nichts Persönliches gegen Sie.

Mir geht es nicht darum Ihnen zu Schaden oder dass Sie Probleme bekommen, alles was ich will ist nur etwas Geld und fertig.

Falls Sie mir die oben genannten 300 € nicht bis zum 27 November 2017 bezahlt haben (Montag um 23:59 Uhr) werde ich Ihre Daten unverzüglich an den Höchstbietenden verkaufen, ich hoffe auf eine Vernünftige und Baldige Lösung von Ihrer Seite.

Phishing-Mails

Das Stehlen von Identitäten und Ausweiskopien ist eine extreme Form des Phishings. Klassische Phishing-Nachrichten sind eine Möglichkeit, wie Betrügerinnen und Betrüger an Ausweiskopien gelangen können.

BEISPIEL AIRBNB

Kriminelle versendeten zum Beispiel erfundene Mails im Namen von Airbnb an zahlreiche Kundinnen und Kunden. Darin wurde behauptet, dass das Konto gesperrt wurde und nun Kopien des Personalausweises, Selfies mit dem Ausweis neben dem Gesicht sowie eine handschriftliche Notiz zur Freischaltung des Kontos notwendig wären. So lautete der Text der E-Mail:

Mein Name ist Miguel von der Trust-Abteilung von Airbnb.

Ihr Airbnb-Konto wurde vorübergehend gesperrt.

Um die Einschränkungen zu entfernen, führen Sie bitte Folgendes aus:

- Beantworten Sie diese E-Mail mit einer Kopie Ihres Personalausweises (beide Seiten).
- Beantworten Sie diese E-Mail mit einem Selfie mit Ihrem Ausweis neben Ihrem Gesicht.
- Beantworten Sie diese E-Mail mit einem Selfie von Ihnen, das eine handschriftliche Notiz mit dem Satz Airbnb und dem heutigen Datum enthält.

Wichtige Anforderungen an Ausweisdokumente:

- Ihr Ausweis muss gültig sein (er darf nicht abgelaufen sein).
- Die Kopie muss gut lesbar sein und die vier Ecken und alle vier Seitenränder enthalten.
- Ihr Foto, Ihr vollständiger Name, Ihr Geburtsdatum, Ihre Unterschrift und die Dokumentennummer müssen sichtbar sein.

Bitte haben Sie Verständnis dafür, dass wir nicht verpflichtet sind, eine Erklärung für die Maßnahmen zu liefern, die gegen Ihr Konto ergriffen wurden. Darüber hinaus haften wir in keiner Weise für die Deaktivierung oder Löschung Ihres Kontos. Airbnb behält sich das Recht vor, diesbezüglich die endgültige Entscheidung zu treffen, und wir werden diese Entscheidung zu diesem Zeitpunkt beibehalten.

Wir werden uns mit Ihnen in Verbindung setzen, falls sich in Zukunft etwas ändert. Bis dahin können wir Sie jedoch nicht weiter bei Ihren Kontoproblemen unterstützen. Weitere Informationen finden Sie in unserer Hilfe: www.airbnb.com/help/article/432

Miguel
www.airbnb.com/help

Kleinanzeigenbetrug

Auch im Bereich des Privateinkaufs kann die Identität von Opfern gestohlen werden. Die Betrügerinnen und Betrüger bieten dafür verschiedene Waren auf Kleinanzeigen-Plattformen an. Meldet sich ein Opfer, wird die genaue Kaufabwicklung besprochen und anschließend eine Ausweiskopie verlangt. Den Wunsch nach der Ausweiskopie begründen die Kriminellen beispielsweise

damit, dass sie beim Verkauf von Waren bereits schlechte Erfahrungen gemacht haben und sich vor kriminellen Käuferinnen und Käufer schützen wollen. Sobald die vermeintlichen Verkäuferinnen oder Verkäufer über die Ausweiskopie ihrer Opfer verfügen, ist keine Kontaktaufnahme mehr mit diesen möglich.

Eine ähnliche Masche wird auch bei der Wohnungssuche angewandt. Schauen sich die Suchenden in Kleinanzeigenportalen um, kann es passieren, dass – neben anderen Dokumenten – auch eine Ausweiskopie verlangt wird. Die vermeintlichen Vermieterinnen und Vermieter erklären in den betrügerischen Inseraten, dass durch einen Identitätsnachweis auch die Chance auf die jeweilige Wohnung erhöht wird.

Wie schützt man sich vor Identitätsdiebstahl?

Die Auflistung der verschiedenen Maschen, mit denen Kriminelle an Identitäten und Ausweiskopien kommen wollen, zeigt, dass dieser Betrug sehr vielfältig ist. Das Problem dabei: Es kann durchaus vorkommen, dass Nutzerinnen und Nutzer online ihre Identität mittels einer Ausweiskopie nachweisen müssen. Dennoch sollte immer überlegt werden, wie nachvollziehbar das Verlangen einer Ausweiskopie ist. Beim Privatkauf oder bei Stellenausschreibungen ist das Versenden eines Reisepasses oder Ähnlichem eher unüblich und sollte daher stutzig machen. Dass Airbnb oder andere Internet-Dienstleister einen Ausweis benötigen, kann allerdings durchaus vorkommen. In diesen Fällen sollte die Kommunikation jedoch wie üblich über die Plattform selbst erfolgen. Um auf der sicheren Seite zu sein, kann die Ausweiskopie so verändert werden, dass Betrügerinnen und Betrüger mit dieser nichts anfangen können:

- **Wasserzeichen hinzufügen:** Mithilfe eines Bildbearbeitungsprogramms können Ausweise mit einem Wasserzeichen versehen werden. Dieses Wasserzeichen soll darüber Auskunft geben, dass es sich um eine Kopie handelt, welchem Zweck die Kopie dient, für wen sie bestimmt ist und wann sie erstellt wurde.
- **Informationen schwärzen:** Auf jedem Ausweis gibt es Informationen, die vom Gegenüber nicht gebraucht werden. Dazu zählt zum Beispiel die Ausweisnummer oder die Unterschrift. Diese Informationen können unleserlich gemacht werden, indem sie beispielsweise geschwärzt werden.

Gut zu wissen: Die Watchlist Internet stellt eine Anleitung zur Verfügung, in der erklärt wird, wie eine Ausweiskopie mit einem Wasserzeichen versehen wird:
https://www.watchlist-internet.at/news/detail/News/ausweiskopien-mit-wasserzeichen-versehen/

Wurde man bereits Opfer eines Identitätsdiebstahls, sollte man unbedingt Strafanzeige bei der Polizei erstatten. Sollten Verbrechen im Namen des Opfers begangen werden, wissen die Behörden Bescheid. Außerdem sollten die Betroffenen in regelmäßigen Abständen überprüfen, ob es im Internet ungewöhnliche Einträge zu ihrer Person gibt. Gegebenenfalls kann eine Löschung der unerwünschten Inhalte bei den Betreiberinnen oder Betreibern der Website gefordert werden.

Weiterführende Links:

https://www.watchlist-internet.at/news/verhalten-sie-sich-als-wuerden-sie-ein-echtes-bankkonto-eroeffnen/

https://www.watchlist-internet.at/news/video-identitaetsdiebstahl-mit-gefaelschten-airbnb-mails/

https://www.watchlist-internet.at/news/identitaetsdiebstahl-das-sind-die-gaengigsten-betrugsmaschen/

KLEINANZEIGENBETRUG

Ebay, Willhaben, Shpock und Co. sind beliebt, um gebrauchte Ware entweder günstig zu kaufen oder verkaufen. Doch auch Kriminelle fühlen sich auf diesen Kleinanzeigenportalen wohl, da sie die Anonymität im Internet gezielt nutzen. Dabei können sowohl Käuferinnen und Käufer als auch Verkäuferinnen und Verkäufer zu Opfern werden.

Abb. 6: Kleinanzeigenbetrug

So werden interessierte Käuferinnen und Käufer zu Opfern

Der Vorkasse-Trick, der Treuhand- und der Liquiditätsbetrug sind beliebte Maschen, mit denen Käuferinnen und Käufer zu Opfern des Kleinanzeigenbetrugs werden.

Der Vorkasse-Trick: Kriminelle verkaufen ein Produkt, oftmals handelt es sich dabei um auffallend günstige

Elektronikartikel oder Gebrauchtwagen. Allerdings befinden sich die vermeintlichen Verkäuferinnen oder Verkäufer meist im Ausland. Daher bitten sie um eine Vorabüberweisung per Geldtransferdienst Western Union, per Paysafecard oder Postanweisung. Trotz der Überweisung des Geldes wird die Ware nicht zugestellt. Auf Nachfrage reagieren die Kriminellen mit unterschiedlichen Argumenten, um das Ausbleiben des Produktes zu rechtfertigen. Dabei heißt es zum Beispiel, dass die Ware nicht zugestellt werden konnte, die Adressangabe falsch war oder es Verzögerungen beim Transportunternehmen gibt. Nach einigen Tagen oder Wochen wird nicht mehr auf E-Mails und Rückfragen reagiert, da die Kriminellen wissen, dass die Opfer bei den genannten Zahlungsmethoden keine Möglichkeit mehr haben, das Geld zurückzuholen.

Der Treuhandbetrug: Auch hier geben die Kriminellen vor, dass sie sich im Ausland befinden. Daher wird der Verkauf über ein angeblich neutrales Speditions- bzw. Logistikunternehmen abgewickelt. Dieses soll sowohl den Transport der Ware übernehmen als auch als Treuhänder für die Zahlung auftreten. In Wirklichkeit gibt es das Unternehmen jedoch nicht. Die Betrügerinnen oder Betrüger versprechen, die Ware dem Speditionsunternehmen zu übergeben, sobald das Geld an dieses Unternehmen überwiesen wurde. Die Website und auch etwaige E-Mails, die die vermeintliche Spedition verschickt hat, sind jedoch gefälscht. Das Geld fließt direkt an die betrügerischen Verkäuferinnen und Verkäufer. Die gekaufte Ware wird nie ausgeliefert, eine Rückbuchung ist nicht möglich.

Der Liquiditätsbetrug: Die Kriminellen schlagen vor, Western Union als Treuhandservice zu nutzen. Bei Western Union handelt es sich jedoch um einen Geldtransferdienst, Treuhandservice wird keiner angeboten. Anschließend werden die Opfer aufgefordert, Geld an Familienmitglieder oder gar an sich selbst zu schicken. Auf diese Weise soll die Liquidität der potenziellen Käuferinnen oder Käufer überprüft werden. Die Betrugsopfer werden dabei dazu gebracht, Details zur Transaktion preiszugeben. Mit den Details sowie einem gefälschten Identitätsnachweis gelangen die Kriminellen an den Geldbetrag. Die gekaufte Ware wird nie ausgeliefert, das Geld ist weg.

So werden Verkäuferinnen und Verkäufer zu Opfern

Auch als Verkäuferin oder Verkäufer auf einer Kleinanzeigen-Plattform ist man nicht davor gefeit Kriminellen aufzusitzen. Der Scheckbetrug, der Trick mit der Track-ID und der PayPal-Trick sind gängige Methoden, mit denen Verkäuferinnen und Verkäufer betrogen werden.

Der Scheckbetrug: Die Kriminellen melden sich auf eine Verkaufsanzeige und zeigen sich interessiert. Allerdings erklären sie meist auf Englisch oder in schlechtem Deutsch, dass sie die Ware mit einem Bankscheck zahlen wollen. Der Versand würde außerdem in ein Land außerhalb der EU erfolgen. Kommt der Scheck an, bemerken die Opfer, dass der angegebene Betrag den vereinbarten Kaufpreis deutlich übersteigt. Die Erklärungen dafür sind unterschiedlich: Mal behauptet die Kriminellen, dass dies der „Mindestbetrag" für einen Scheck gewesen sei, dass sie sich verschrieben haben oder der Differenzbetrag für den Transport gedacht sei. Egal, welchen Grund die Kriminellen angeben, läuft es darauf hinaus, dass die Differenz in der Regel per Western Union oder per Auslandsüberweisung rücküberwiesen werden soll.

Das Problem dabei: Wenn der Scheck auf der Bank hinterlegt wird, wird der Betrag zwar sofort gebucht, die Überprüfung, ob der Scheck auch gedeckt ist, dauert aber einige Tage. Stellt sich der Scheck als nicht gedeckt oder gefälscht heraus, wird das Geld wieder vom Konto abgebucht. In diesem Fall bleibt den Betrogenen weder die per Scheck angewiesene Summe noch der überwiesene Differenzbetrag. Schlimmstenfalls wurde in der Zwischenzeit auch noch die Ware versandt und ist nicht mehr rückrufbar.

Der Trick mit der Track-ID: Ohne große Nachfrage wollen die Kriminellen ein Produkt kaufen und bitten sofort um die Kontodaten für eine Überweisung. Nachdem die Bankdaten bekannt gegeben wurden, erhalten die Opfer eine Benachrichtigung von der (vermeintlichen) Bank der Kriminellen: Die Überweisung sei bereits in Auftrag gegeben worden. Bevor das Geld jedoch an die Bank der Opfer weitergeleitet werden könne, würde „zum Schutz beider Seiten" eine Track-ID oder ein Versandbeleg benötigt. Der Versand soll meist in ein Land außerhalb der EU (häufig Senegal oder Nigeria) erfolgen. Nachdem die Ware versandt und der Versandbeleg weitergegeben wurde, bricht der Kontakt aber plötzlich ab und das Geld kommt nie an. Die E-Mails der Bank waren gefälscht, die Ware ist weg.

Der PayPal-Trick: Die Kriminellen wollen ein Produkt kaufen und bestehen darauf, die Zahlung über PayPal abzuwickeln. Zudem befinden sie sich gerade im Ausland, die Ware (meist ein PKW) soll von einem vermeintlichen Transportunternehmen abgeholt werden. Kurze Zeit später erhält das Opfer eine gefälschte E-Mail von PayPal, in welcher der Zahlungseingang bestätigt wird. Der überwiesene Betrag übersteigt jedoch den vereinbarten Kaufpreis deutlich. Die Differenz wird entweder direkt in der gefälschten E-Mail von PayPal oder in einer E-Mail der Kriminellen erklärt: Es handle sich dabei um die Kosten für den Transport. Diese sollen von den Opfern mittels Bargeldtransfer an das Transportunternehmen gezahlt werden. Wird den Anweisungen in der E-Mail gefolgt, verlieren die Opfer das Geld, denn das Transportunternehmen gibt es nicht.

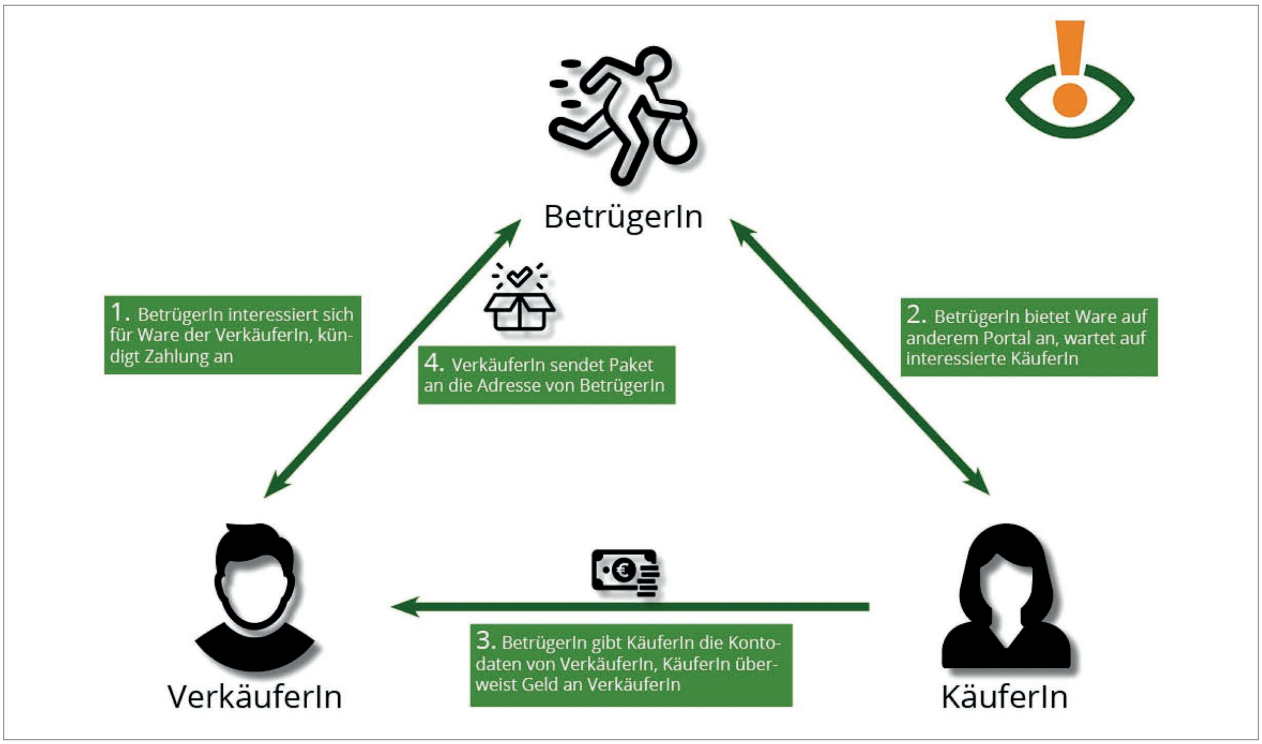


Abb. 7: Dreiecksbetrugsfalle

Sonderfall: Dreiecksbetrug

Eine besonders perfide Betrugsfalle ist der Dreiecksbetrug. Hier werden sowohl Käuferinnen und Käufer als auch Verkäuferinnen und Verkäufer abgezockt. Wie der Name bereits verrät, beim benötigt es drei Personen: eine ehrliche Person (Verkäuferin/Verkäufer), der eine meist hochwertige Ware in einem Kleinanzeigenportal anbietet, eine Person (Käuferin/Käufer), die Interesse an dieser Ware hat und bereit ist dafür zu bezahlen, und dazwischen eine Betrügerin oder einen Betrüger, der die Ware ebenfalls will – jedoch ohne dafür zu bezahlen. Um das zu erreichen, wendet die Betrügerin oder der Betrüger ebenso einen Trick an, der für die ehrliche Verkäuferin/den ehrlichen Verkäufer genauso wenig nachvollziehbar ist wie für die ehrliche Käuferin/Käufer:

- Die Betrügerin/Der Betrüger sucht auf Kleinanzeigenportalen nach einer Ware. Sie/Er bekundet gegenüber der ehrlichen Verkäuferin/dem ehrlichen Verkäufer Interesse und kündigt an, den Betrag für die Ware in den nächsten Tagen über PayPal oder auf das Bankkonto zu überweisen.
- Gleichzeitig kopiert die Kriminelle/der Kriminelle die Anzeige der ehrlichen Verkäuferin/des ehrlichen Verkäufers und stellt das Angebot auf eine andere Kleinanzeigen-Plattform. Die Kriminelle/Der Kriminelle wartet, bis sich eine ehrliche Käuferin/ein ehrlicher Verkäufer meldet und die Ware kaufen möchte.
- Die Kriminelle/Der Kriminelle gibt der Käuferin/dem Käufer die Kontodaten der Verkäuferin/des Verkäufers. Diese überweist das Geld an die Verkäuferin/den Verkäufer.
- Die Verkäuferin/Der Verkäufer hat das Geld erhalten und versendet daher die Ware, allerdings hat die Betrügerin/der Betrüger seine eigene Adresse genannt. Er erhält also das Paket mit der Ware, die von der ehrlichen Käuferin/dem ehrlichen Käufer bezahlt wurde. Die Käuferin/Der Käufer, die/der die Ware bezahlt hat, wartet hingegen vergebens auf ihr/sein Paket.

10 Tipps, um sich vor Kleinanzeigenbetrug zu schützen

1. Bei Verkäufen und Überweisungen ins Ausland ist besondere Vorsicht geboten.
2. Es sollte kontrolliert werden, ob Beträge tatsächlich gutgeschrieben wurden und im Zweifelsfall bei der Bank oder dem Zahlungsdienstleister nachgefragt werden.
3. Bei überhöhten Zahlungen gilt es skeptisch zu sein.
4. Es sollten die Kommunikationsmöglichkeiten der jeweiligen Kleinanzeigen-Plattform genutzt werden. Besteht das Gegenüber auf externem Mail- oder WhatsApp-Kontakt, kann dies ein Hinweis auf Betrug sein.
5. Der Kauf bzw. Verkauf sollte idealerweise persönlich abgewickelt werden. Direkt bei der Übergabe zu bezahlen stellt die sicherste Variante dar.
6. Achtung auch bei verdächtig günstigen Angeboten.
7. Stimmt die Sprache beim ursprünglichen Angebot nicht mit der späteren Kommunikation überein, sollte lieber Abstand genommen werden. Gleiches gilt auch für Vorwahlen bei Handynummern.
8. Vorsicht ist außerdem geboten, wenn der angegebene Name in der Kleinanzeige nicht mit dem Namen der E-Mail-Adresse, mit dem Namen der kontoführ-

renden Person oder mit dem Empfangsnamen des Pakets übereinstimmt.

9. Auch die Versandadresse sollte mit der Adresse des PayPal-Kontos oder anderer Zahlungsdaten verglichen werden. Unterscheiden sich die beiden Adressen, ist das ein Alarmsignal.
10. Beim Kleinanzeigenverkauf dürfen keine Ausweiskopien ausgetauscht werden. Derartige Kopien werden von Kriminellen häufig für weitere Verbrechen unter dem Deckmantel der falschen Identität missbraucht.

Betrug bei der Wohnungssuche

Zentrale Lage in der Wiener Innenstadt. Eingerichtet mit neuesten Möbeln und Geräten. 87m² und dazu noch eine Terrasse oder einen Balkon. Das Beste daran: Die Miete beträgt nur 450 Euro monatlich, weit unter dem Durchschnitt also. Solche privaten Wohnungsinserate finden sich immer wieder auf Immobilien- und Kleinanzeigenplattformen wie immowelt.at, immobilienscout24.at oder willhaben.at. Meist stellen sich diese Traumwohnungen aber als Betrug heraus und sind tatsächlich zu schön, um wahr zu sein.

Wie funktioniert die Masche?

Wohnungssuchende nehmen Kontakt mit vermeintlichen Vermieterinnen oder Vermietern auf und erhalten rasch die Rückmeldung, dass die privat inserierte Wohnung noch zu haben ist. Gleichzeitig stellen sich die Vermieterinnen und Vermieter vor und erklären, aus welchem Grund die Wohnung zu haben ist.

Bald darauf wird klar, dass sich die betrügerischen Vermieterinnen oder Vermieter im Ausland befinden. Daher soll die Abwicklung über Airbnb stattfinden. Um die Immobilie besichtigen zu können, soll eine Kaution an Airbnb überwiesen werden. Sollten sich die Opfer nach der Besichtigung gegen die Wohnung entscheiden, bekommt man das Geld wieder zurück.

In einem letzten Schritt erhalten die Opfer einen Link, der zu einer gefälschten Airbnb-Seite führt. Diese Nachrichten werden von E-Mail-Konten gesendet, die scheinbar von Airbnb sind. Im Absender-Feld heißt es dann zwar Airbnb, die tatsächliche E-Mail-Adresse lautet aber zum Beispiel xyname@airbnb-musterseite.com. Sie ist gefälscht und stammt nicht von airbnb.com. In dieser Mail wird ein Link geschickt, der auf eine (ebenfalls gefälschte) Airbnb-Seite führt. Dort wird man aufgefordert, die Kaution zu bezahlen. Auch wenn das geforderte Geld bezahlt wurde, gibt es weder eine Besichtigung noch das Geld zurück.

> **Tipp:** Für die Besichtigung einer Wohnung sollte nie eine Kaution bezahlt werden. Spätestens, wenn die vermeintlichen Vermieterinnen oder Vermieter vorschlagen, die Besichtigung über Airbnb abzuwickeln, sollte man sich von der „angeblichen" Traumwohnung verabschieden.

Weiterführende Links:

https://www.watchlist-internet.at/news/detail/News/die-tricks-der-kleinanzeigen-betrueger-teil-1/

https://www.watchlist-internet.at/news/detail/News/die-tricks-der-kleinanzeigen-betrueger-teil-2/

https://www.watchlist-internet.at/news/detail/News/so-schuetzen-sie-sich-vor-kleinanzeigen-betrug/

https://www.watchlist-internet.at/news/dreiecksbetrug-bei-kleinanzeigen/

PHISHING

Phishing ist ein Begriff, der sich aus dem Englischen für „password harvesting" (Passworte sammeln/ernten) und „fishing" (angeln, fischen) zusammensetzt. Unter Phishing versteht man also das Angeln nach Passwörtern mit bestimmten Ködern verstehen. Dazu werden betrügerische Nachrichten von Kriminellen verschickt, in denen die Empfängerinnen und Empfänger unter unterschiedlichsten Vorwänden (Ködern) aufgefordert werden, geheime Daten bekanntzugeben.

Wie gehen die Betrügerinnen und Betrüger vor?

Meist geben sich die Betrügerinnen und Betrüger als ein bekanntes Unternehmen aus. Besonders beliebt sind dabei Banken, Zahlungsdienstleister oder Online-Plattformen. Im Namen dieses Unternehmens werden an zahlreiche Menschen Nachrichten verschickt. Das können E-Mails oder SMS sein, aber auch Chatnachrichten, die über einen Messenger oder über soziale Netzwerke versandt werden.

Der Inhalt dieser Nachrichten kann sehr unterschiedlich sein. Das Ziel ist jedoch immer das Gleiche: Die Kriminellen versuchen mithilfe von glaubwürdig klingenden Argumenten an sensible Daten zu kommen. Mit den betrügerischen Nachrichten wird ein Link (manchmal auch ein Dateianhang in Form eines Formulars) mitgeschickt, der zu einer sogenannten Phishing-Seite führt: Eine Seite, die der Website des nachgeahmten Unternehmens ähnelt und auf der sich die Opfer einloggen und/oder ihre Kreditkartendaten eingeben sollen.

Vorwände, mit denen die Betroffenen geködert werden, um ihre Daten preiszugeben, können zum Beispiel sein:

- **„Aktualisieren Sie Ihre Zahlungsinformationen“:** Im Namen von Netflix schreiben Kriminelle, es gebe Probleme mit der Rechnung, daher müssten die Zahlungsinformationen aktualisiert werden. Der mitgeschickte Link führt zu einer gefälschten Netflix-Seite, auf der die Kreditkartendaten eingegeben werden sollen.

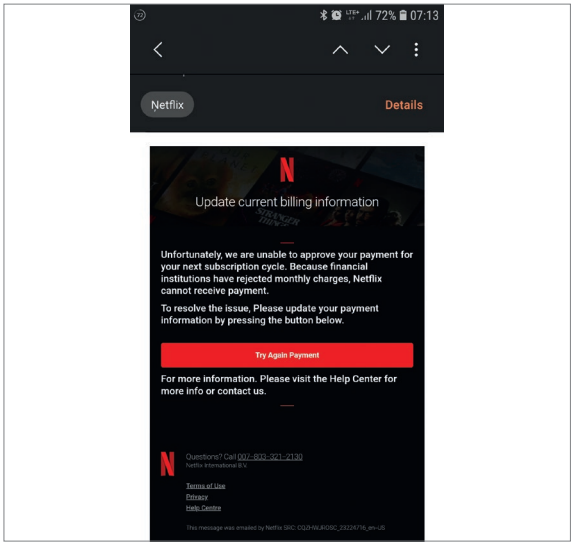


Abb. 8: Netflix-Phishing-Mail

- **„Kundenmitteilung“:** Im Namen von Banken wie der BAWAG P.S.K. oder der Raiffeisenbank werden die Opfer dazu aufgefordert eine Sicherheits-App zu installieren, um das Konto weiterhin verwenden zu können. Die Links in den Nachrichten, die sowohl per Mail als auch per SMS verschickt werden, führen zu gefälschten Login-Seiten. Melden sich die Opfer mit ihren Zugangsdaten auf dieser Seite an, landet das Passwort direkt bei den Kriminellen.

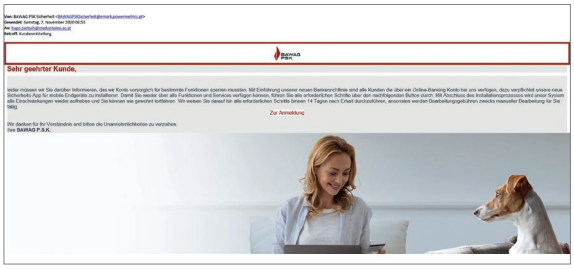


Abb. 9: BAWAG P.S.K.-Phishing-Mail

- **„Antworten Sie auf die offene Anfrage: 12345XYZ“:** Kriminelle versenden Nachrichten im ebay-Design mit dem Hinweis, dass eine interessierte Person von einem Kauf zurücktreten wolle und man dieser Person antworten solle. Dafür kann man direkt auf einen Link klicken. Dieser führt zu einer gefälschten ebay-Website, auf der man sich anmelden muss. Dadurch erhalten die Kriminellen Zugang zum betroffenen ebay-Konto und können dieses für betrügerische Angebote auf ebay nutzen.

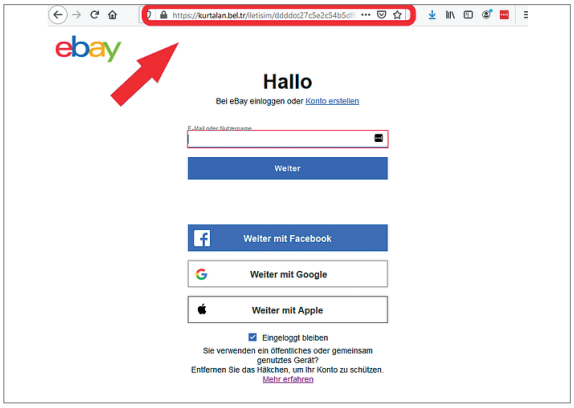


Abb. 10: ebay-Phishing-Mail

- **„Ihr Paket [006232013] steht in Terminal 4 noch aus“:** Per SMS geben sich Kriminelle als Post aus und versenden Lieferbenachrichtigungen. Um das vermeintliche Paket zu erhalten, müssen jedoch noch die Daten bestätigt werden. Zu diesen Daten zählen auch die Kreditkartendaten. Diese weit verbreitete Masche führt nicht nur zum Diebstahl der persönlichen Daten, sondern auch in die Abo-Falle, denn durch die Dateneingabe wird unabsichtlich ein teures Abonnement abgeschlossen.

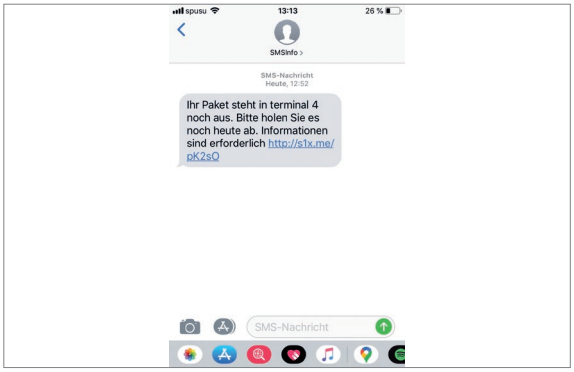


Abb. 11: Post-Phishing-Mail

- **„Aufgrund eines Fehlers unserer Rechnungsabteilung wurde Ihnen das Doppelte Ihrer letzten Rechnung in Rechnung gestellt“:** So heißt es in der betrügerischen E-Mail, die angeblich von Magenta kommt. Die Empfängerinnen und Empfänger sollen auf einen Link klicken, um eine Rückerstattung zu beantragen. Dort sollen sowohl die Zugangs- als auch die Kreditkartendaten eingegeben werden.

Abb. 12: Magenta-Phishing-Mail

Das sind nur wenige Beispiele einer großen Bandbreite von Phishing-Nachrichten. Die Watchlist Internet informiert über aktuelle Phishing-Versuche unter https://www.watchlist-internet.at/phishing-datendiebstahl/.

Phishing-Versuche auf sozialen Netzwerken

Auch auf sozialen Netzwerken wie Facebook und Instagram werden Phishing-Versuche zunehmend beliebter. Die Betrügerinnen und Betrüger, die hinter diesen Phishing-Versuchen stecken, verfolgen dabei das Ziel einen Facebook- oder Instagram-Account zu übernehmen. Durch diese Accounts erhalten Kriminelle nicht nur eine Vielzahl an Informationen über die jeweiligen Personen, sondern können die Freundinnen und Freunde des kompromittierten Accounts gezielt angreifen, indem gefährliche Nachrichten versendet oder schädliche Beiträge verfasst werden. Da die Followers dem übernommenen Account vertrauen, ist es für Cyberkriminelle auf diesem Weg einfach Schadsoftware oder Links zu verschiedenen betrügerischen Seiten zu verbreiten.

Wie auch bei anderen Phishing-Versuchen verfassen die Betrügerinnen und Betrüger dafür Nachrichten mit einem Link zu einer nachgebauten Login-Seite des jeweiligen Netzwerkes. Dafür geben sie sich als Facebook oder Instagram aus und bitten die Nutzerinnen und Nutzer sich auf der mitgeschickten Phishing-Seite einzuloggen. Es kommt aber auch vor, dass von bereits kompromittierten Konten Phishing-Nachrichten versendet werden.

Wie schützt man sich vor Phishing-Versuchen?

Kriminelle geben sich immer mehr Mühe, wenn es um Phishing geht: Die Vorwände wirken glaubwürdiger und die nachgeahmten Nachrichten und Websites ähneln dem Original immer mehr. Für Internet-Nutzerinnen und Internet-Nutzern wird es dadurch zunehmend schwieriger, Betrug eindeutig als solchen zu erkennen. Dennoch gibt es Möglichkeiten Phishing-Nachrichten und -Seiten zu entlarven:

- **Absender prüfen:** Oftmals lässt sich eine Phishing-Nachricht allein durch den Absender entlarven. Passt die E-Mail-Adresse zum Inhalt der Nachricht? Ein genauer Blick auf den Absender zeigt zum Beispiel, dass die BAWAG P.S.K. wohl kaum eine Nachricht von der E-Mail-Adresse „no-replay@commetnauto.com“ schicken wird. Gleiches gilt beim Versenden von SMS: Seriöse Unternehmen schicken keine wichtigen Nachrichten mit unterdrückter Nummer oder unter dubiosem Namen.
- **Inhalt hinterfragen:** Phishing-Nachrichten wirken manchmal nur auf den ersten Blick plausibel, daher sollten sich die Empfängerinnen und Empfänger genauer mit dem Inhalt beschäftigen. Hat die betroffene Person ein Nutzerkonto beim jeweiligen Unternehmen? Kommt die Nachricht unerwartet? Werden sensible Daten abgefragt? Seriöse Unternehmen wie Banken, Onlineshops oder Kleinanzeigen-Plattformen fragen keine Kundendaten per E-Mail ab. Solche Nachrichten sollten daher ignoriert werden.
- **Auf Grammatik und Rechtschreibung achten:** Auch Grammatik- und Rechtschreibfehler können ein Hinweis darauf sein, dass es sich um eine Phishing-Nachricht handelt. Natürlich können auch seriösen Unternehmen Fehler unterlaufen, ist die Nachricht jedoch voller Fehler, handelt es sich wahrscheinlich um Betrug.
- **Webadresse identifizieren und überprüfen:** Die meisten Phishing-Nachrichten beinhalten Links. Diese können oft daran erkannt werden, dass der Text blau oder unterstrichen ist. Manchmal sind die Links auch in Buttons oder Bildern integriert. Wird ein solcher Link berührt – ohne ihn anzuklicken – erscheint die Webadresse (auch URL genannt) entweder ganz unten im Mailprogramm oder direkt neben dem jeweiligen Link. Wurde die Webadresse identifiziert, sollte diese genau überprüft werden: Stimmen der (vermeintliche) Absender und der Inhalt der Nachricht mit der Webadresse überein? Gibt es Fehler in der Webadresse (zum Beispiel bawagpks.at statt bawagpsk.at)?
- **Unternehmen direkt kontaktieren:** Auch wenn die obigen Schritte befolgt wurden, kann nach wie vor Unsicherheit bestehen. Da die Kriminellen immer überzeugender werden, sind manche Phishing-Nachrichten kaum als solche zu erkennen. Daher sollte im Zweifelsfall das jeweilige Unternehmen direkt kontaktiert werden: Ein Anruf oder eine E-Mail an die gewohnte E-Mail-Adresse kann rasch klären, ob die Nachricht tatsächlich vom Unternehmen stammt.
- **Zwei-Faktor-Authentifizierung aktivieren:** Um sich auf sozialen Netzwerken vor Phishing-Versuchen zu schützen, ist es sinnvoll die sogenannte „Zwei-Faktor-Authentifizierung“ oder „zweistufige Authentifizierung“ zu verwenden. Dadurch reicht das Passwort nicht mehr aus, um sich anzumelden. Das macht auch Kriminellen, die ein Konto übernehmen wollen, das Leben schwer. Saferinternet.at stellt Schritt-für-Schritt-Anleitungen für die Aktivierung der Zwei-Faktor-Authentifizierung auf Facebook und Instagram zur Verfügung.

(!) Gut zu wissen: Eine Webadresse besteht immer aus einer Domain und aus einer Top-Level-Domain. Manchmal hat eine Domain auch Unterseiten. In diesem Fall besteht eine Webadresse zusätzlich aus einer Subdomain. Dies ist beispielsweise auch bei der Webadresse für den Login bei der BAWAG P.S.K. der Fall:
ebanking.bawagpsk.at

Subdomain Domain Top-Level-Domain

Diesen Aufbau nutzen Kriminelle oftmals, um zu verwirren. So könnte eine nachgebaute und betrügerische Seite der BAWAG P.S.K. folgendermaßen lauten: ebanking-bawagpsk.login.at

Die Subdomain lautet hier ebanking-bawagpsk. Dieser Teil ist jedoch nur eine Unterseite der Website login.at. Die geschickte Zusammensetzung von Subdomain und Domain vermittelt den Eindruck, als würde es sich tatsächlich um die Login-Seite der BAWAG P.S.K. handeln. Die Domain (login.at) kann auch als Wer-Bereich einer Webadresse bezeichnet werden, da sie einen Hinweis darauf gibt, wem diese Seite zuzuordnen ist. Anders ausgedrückt: Man befindet sich nicht auf der Seite der BAWAG P.S.K. (bawagpsk.at), sondern auf der Seite login.at. Mit der Bank hat diese nichts zu tun.

Eine weitere beliebte Masche ist das Verwenden von Domains, die mit dem Wer-Bereich fast übereinstimmen. Demnach könnte eine Phishing-Seite auch folgendermaßen aussehen:
ebanking.bawagpks.at
ebanking.bawapsk.at
ebanking.bagawpsk.at

Das Karlsruher Institut für Technologie stellt leicht verständliche Erklärvideos zur Verfügung, die darauf eingehen, wie Absender geprüft und gefährliche Links erkannt werden können: https://secuso.aifb.kit.edu/1047.php

Wie minimiert man den Schaden nach einem erfolgreichen Phishing-Versuch?

Wurden die Daten bereits eingegeben, muss schnell gehandelt werden. Folgende Schritte sind dafür zentral:

- **Unternehmen kontaktieren:** Das Unternehmen (die Bank, den Kreditkartenanbieter, den Shop-Betreiber), das als vermeintlicher Absender der Phishing-Nachrichten angegeben ist, muss sofort kontaktiert werden. Nachdem dort die Situation erklärt wurde, kann gemeinsam das weitere Vorgehen zur Schadensabwehr besprochen werden.
- **Bankkonten und Karten sperren:** Wurden Bankdaten, TANs oder Kreditkartendaten bekanntgegeben, müssen die entsprechenden Konten, Online-Zugänge oder Kreditkartendaten gesperrt werden, damit Unbefugte keinen Zugriff haben.
- **Passwörter ändern:** Handelt es sich um Accounts bei Onlineshops, Kleinanzeigen-Plattformen oder auf sozialen Netzwerken, gilt es sich rasch in den entsprechenden Account einzuloggen und das Passwort zu ändern. Ist kein Login mehr möglich, da die Kriminellen das Passwort bereits geändert haben, kann der Betreiber der Website kontaktiert werden, um eine umgehende Deaktivierung des entsprechenden Accounts zu fordern.
- **Phishing-Seiten melden:** Um andere Nutzerinnen und Nutzer vor Phishing-Versuchen zu warnen, können betrügerische Seiten bei Google gemeldet werden (https://safebrowsing.google.com/safebrowsing/report_phish/?hl=de). Nachdem eine Meldung abgesendet wurde, kommt es zur Prüfung der jeweiligen Website. Handelt es sich um Betrug, erhalten Personen, die diese Website aufrufen, eine Warnung. So wird verhindert, dass diese ihre Daten auf den Phishing-Seiten eingeben.

Weiterführende Links:

https://www.watchlist-internet.at/news/detail/News/wenn-sie-in-die-phishing-falle-getappt-sind/

https://www.watchlist-internet.at/news/detail/News/so-schuetzen-sie-sich-vor-phishing-versuchen/

https://www.watchlist-internet.at/news/detail/News/im-webbrowser-vor-phishing-attacken-schuetzen/

https://www.watchlist-internet.at/news/netflix-kundinnen-aufgepasst-betruegerische-e-mails-im-umlauf/

https://www.watchlist-internet.at/news/kriminelle-versuchen-zugangsdaten-zum-online-banking-zu-klauen/

https://www.watchlist-internet.at/news/vorsicht-bei-gefaelschten-nachrichten-von-smsinfo-zu-paketlieferungen/

https://www.watchlist-internet.at/news/e-mail-doppelte-abbuchung-ihrer-magenta-rechnung-ist-fake/

SCAMMING

Scamming (dt. betrügen) beschreibt eine beliebte Betrugsform im Internet, die Kriminelle nutzen, um an schnelles Geld zu gelangen. Sie versprechen ihren Opfern Erbschaften, Millionengewinne, günstige Kredite oder Wohnungen, spielen ihnen eine Notlage oder Liebe vor und drängen sie zu einer Überweisung. Es handelt sich ausnahmslos um leere Versprechen und das Geld landet in den Taschen von Kriminellen.

Scamming-Betrugsmaschen erfolgen meist nach einem ähnlichen Schema:

- Opfer werden unerwartet per E-Mail oder Chat kontaktiert und ihnen wird unter einem Vorwand eine hohe Geldsumme versprochen.

- Opfer werden auf höchst emotionale Weise um Geld gebeten oder erpresst.
- Opfer müssen für eine bestimmte Leistung vorab etwas überweisen.

Im Grunde können fünf Scamming-Arten, die in abgewandelter Form immer wieder auftreten, unterschieden werden: Erpressungs-E-Mails, Erbschafts- oder Gewinnversprechen, Love-Scamming, Scamming auf dem Wohnungsmarkt und betrügerische Kreditkartenplattformen.

Erpressungs-E-Mails

In einem Erpressungs-E-Mail werden Empfängerin/Empfänger – wie der Name bereits vermuten lässt – anhand erfundener Anschuldigungen erpresst. Erpressungs-E-Mails sind in unterschiedlichen Varianten im Umlauf und werden wahllos und massenhaft versendet.

Variante 1

Die Kriminellen behaupten, sie hätten den Computer der Empfängerin bzw. des Empfängers gehackt, sie beim Surfen auf einer Pornoseite ertappt, die Webcam aktiviert und sie beim Masturbieren gefilmt. Damit dieses Videomaterial nicht veröffentlicht wird, sollten die Betroffenen Bitcoins überweisen. Um Opfer zu einer Überweisung zu bringen, sind derartige E-Mails meist sehr vulgär, einschüchternd und aggressiv formuliert, oftmals wird auch sehr ausführlich geschildert, wie der Computer bzw. die Webcam der Empfängerin bzw. des Empfängers angeblich gehackt wurden. Um einen vermeintlichen Hackangriff möglichst glaubhaft erscheinen zu lassen, behaupten Kriminelle Zugriff auf Passwörter der Empfängerin bzw. des Empfängers zu haben. Beispielhaft wird auch ein Passwort genannt. Dieses Passwort wurde jedoch nicht durch einen Virus oder Hackangriff auf den Computer der Opfer erspäht, sondern weil die Kriminellen eine Datenbank mit Nutzerdaten besitzen. Eine weitere Methode, einen Hackangriff plausibel erscheinen zu lassen, ist, dass Kriminelle den E-Mail-Kopf so manipulieren, dass es aussieht, als hätte der Hacker das E-Mail vom Account des Opfers an das Opfer selbst versendet.

Watchlist Internet: Bitcoin Erpressungs-E-Mail von mir selbst
Watchlist Internet: Bitcoin-Erpressungsmail mit Nacktbildern
Watchlist Internet: Video: Erpressungs-Mails

Variante 2

Eine weitere Variante von Erpressungs-E-Mails richtet sich speziell an Unternehmen oder Websitebetreiberinnen bzw. -betreiber. Darin wird behauptet, dass die Firmenwebsite gehackt und vertrauliche Daten bzw. Kundendaten gestohlen wurden. Um möglichst bedrohlich zu wirken und Opfer zu einer Überweisung zu nötigen, beschreiben die Kriminellen oftmals Schritt für Schritt, was passiert, wenn nicht überwiesen wird. Beispielsweise werden angeblich alle Kundinnen und Kunden über die vermeintliche Sicherheitslücke informiert, die Website unwiderruflich zerstört, das Firmenimage ruiniert oder das Google-Ranking der Website manipuliert.

Oft wird auch damit gedroht, dass, dass im Geschäftsgebäude eine Bombe gezündet wird, wenn nicht innerhalb einer gewissen Zeitspanne Bitcoins überwiesen werden.

Watchlist Internet: Erpressungs-Mail mit Bombendrohung massenhaft versendet
Watchlist Internet: „Ihre Site wurde gehackt“: Unternehmen werden per Mail erpresst

Erbschafts- oder Gewinnversprechen

Die Kriminellen kontaktieren ihre Opfer meist per E-Mail, Chat oder SMS. Sie geben sich als Verwaltungsperson eines Millionenerbes, Investor/in, Bankmitarbeiter/in, Lotterie-Mitarbeiter/in, Spendenorganisationen, Kreditanbieter/in oder Kommunikationsbeauftragte/r einer großen Firma aus. Man stellt sich kurz vor und verspricht hohe Geldbeträge. Derartige Nachrichten werden nicht an eine bestimmte Person, sondern massenhaft und wahllos an alle verfügbaren E-Mail-Adressen versendet. Um das Geld zu erhalten, muss nur auf die Nachricht geantwortet und persönliche Daten wie Name, Anschrift, Telefonnummer oder Ausweiskopien müssen übermittelt werden. Auf eine Antwort folgen dann weitere Nachrichten, in denen Details zur Abwicklung der angeblichen Überweisung geklärt werden. Den Opfern wird erklärt, dass die Überweisung einer derart hohen Summe mit einem bürokratischen Verwaltungsaufwand verbunden sei und dafür zuvor Kosten entstünden: Kosten für Sicherheitszertifikate, notarielle Beglaubigungen, Spesen etc. – Kriminelle sind durchaus kreativ, um Opfer zu einer Vorabzahlung zu überreden.

Kriminelle legen sich beim Vorschussbetrug oftmals richtig ins Zeug. Um Opfer zu einer Überweisung zu bringen, wird sehr viel kommuniziert, sogar Websites werden erstellt oder Fake-Finanz- und Bankberater/innen involviert. Nach erfolgter Überweisung wird jedoch kein Geld übermittelt, sondern es werden lediglich weitere Vorwände aufgetischt, warum nochmals Geld überwiesen werden muss.

Watchlist Internet: Vorschussbetrug: Ein Opfer berichtet …
Watchlist Internet: Gewinnversprechen von Coca-Cola in Höhe von 1 Million US-Dollar ist Scam

Love-Scamming

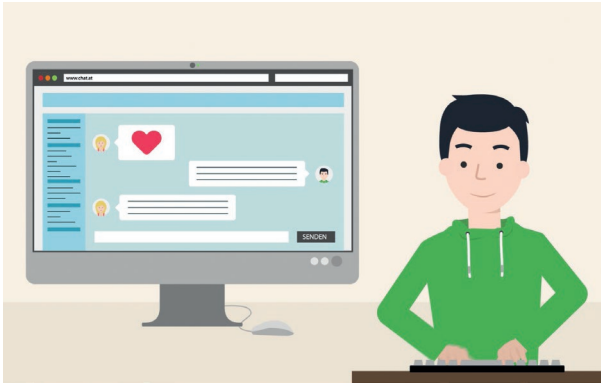


Abb. 13: Love-Scamming

Romance- bzw. Love-Scammer sind überall dort zu finden, wo eine Kontaktaufnahme sehr einfach ist. Das kann eine Dating- oder Partnerbörse sein, das können soziale Medien wie Facebook oder Instagram sein, aber auch verschiedene Nachrichten-Tools, Messenger oder Chat-Plattformen.

Auf Fake-Profilen geben sich Kriminelle als erfolgreiche Manager oder Soldaten aus und chatten über einen längeren Zeitraum mit ihren Opfern. Ist das Opfer ein heterosexueller Mann, geben sich die Kriminellen als attraktive Frau aus. Sie sprechen rasch von der großen Liebe, schmieden Zukunftspläne, erzählen Details aus ihrem Alltag und wollen auch alles Mögliche von ihrem Gegenüber wissen. Ein reales Treffen kommt jedoch selten zustande, stattdessen wird nach einiger Zeit um Geld gebeten. Die Forderungen nach Geldüberweisungen werden dabei meist von emotionalen Geschichten begleitet: Ein Todesfall in der Familie, eine schwere Krankheit oder ein Unfall, der plötzliche Jobverlust, unbeglichene Hotelrechnungen oder Probleme mit Behörden können Gründe sein, wieso die Betrügerinnen und Betrüger plötzlich Geldnot haben. Genauso kann es aber auch sein, dass sie das Geld brauchen, um vom Ausland zu den Opfern zu fliegen, um diese endlich kennenzulernen.

Watchlist Internet: Vorsicht, wenn Ihr Tinder-Match über lukrative Investitionsmöglichkeiten spricht
Watchlist Internet: Wahre Liebe oder Betrug? So finden Sie es heraus!

Scamming auf dem Wohnungsmarkt

Kriminelle inserieren günstige Miet- und Eigentumswohnungen, Häuser und Grundstücke auf bekannten Immobilienplattformen. Dabei handelt es sich um absolute Traumhäuser, -wohnungen oder -grundstücke in bester Lage zu einem überaus günstigen Preis.

Der Haken: Interessierte sollen bereits vor der Besichtigung eine Kaution überweisen. Die betrügerischen Vermieterinnen und Vermieter erklären, dass sie aus einem bestimmten Grund gerade im Ausland sind und die Besichtigung nicht selbst abwickeln können. Daher beauftragen sie angeblich ein Treuhandunternehmen oder Airbnb als vertrauenswürdigen Vermittlungskontakt, der die Besichtigung organisiert und Vorabzahlungen verwaltet. An dieses Unternehmen sollte dann die Kaution vorab überwiesen werden. Sollten sich die Interessentinnen und Interessenten nach der Besichtigung gegen die Wohnung entscheiden, bekommen sie das Geld selbstverständlich wieder zurück. Tatsächlich gibt es weder eine Besichtigung noch das Geld zurück! Um Opfer zu einer Vorabzahlung zu bewegen, wird sehr häufig auch eine Website des vermeintlichen Treuhandunternehmens bzw. eine gefälschte Airbnb-Website erstellt. Und: Airbnb organisiert weder Besichtigungstermine noch verwaltet die Firma Kautionen. Mit der Einbeziehung von Airbnb als Verwalter der Kaution sollte lediglich Vertrauen gestiftet werden.

Watchlist Internet: Gerade auf Wohnungssuche? Dann sollten Sie sich vor gefälschten Inseraten in Acht nehmen!
Watchlist Internet: Sie vermieten Zimmer? – Dann sollten Sie diese Betrugsmasche kennen!

Betrügerische Kreditplattformen

Betrügerische Kreditplattformen sind Websites, die einen günstigen Kredit versprechen. Die Kriminellen hinter der Website missbrauchen dabei sehr häufig Logos bekannter Banken oder Kreditinstitute, um Vertrauen zu stiften. Potenzielle Kreditnehmerinnen und Kreditnehmer müssen für einen Kredit zunächst eine Onlineanfrage ausfüllen. Dabei werden zahlreiche persönliche Daten (Name, Adresse, E-Mail-Adresse, Telefonnummer) erfragt. Daraufhin werden Opfer von den Kriminellen kontaktiert, um ihnen die weiteren Schritte zum Erhalt des Kredits zu erklären. So wird beispielsweise erklärt, dass vorab eine kleine Gebühr bezahlt werden muss (Versicherungsgebühr, Aktivierungsgebühr, Antigeldwäschegebühr, Kautionshinterlegung, Anwaltskosten etc.). In Wahrheit wird jedoch niemals ein Kredit vergeben. Das Spiel mit weiteren Kosten setzt sich so lange fort, bis Opfer Betrugsverdacht schöpfen und nichts mehr einzahlen.

Watchlist Internet: Betrügerische Kredite von Continental Bank und Eran Finance!
Watchlist Internet: Vorsicht vor knuth-kredit.online: Vorschussbetrug statt Kreditvergabe

Tech-Support-Scams

Ein Tech-Support-Scam ist eine Betrugsmasche, bei der sich Kriminelle als Service-Mitarbeiterinnen und Servicemitarbeiter von Microsoft oder Apple ausgeben und ein Computerproblem vortäuschen. Die Kontaktaufnahme erfolgt entweder durch die Kriminellen per Telefon oder die Opfer rufen aufgrund eines Pop-ups selbst bei einer vermeintlichen Service-Stelle an. In beiden Fällen wird eine Fernwartungssoftware installiert, um Zugangsdaten zu erspähen, Schadsoftware zu installieren oder Daten zu löschen oder zu stehlen.

Opfer werden immer aus Angst vor einem möglichen Schaden am eigenen Computer in die Falle gelockt. Kriminelle behaupten, dass es ein Problem mit dem Computer oder Laptop gebe, welches mithilfe einer Fernwartung behoben werden könne. In die Falle tappen Opfer meist über zwei Wege: Anrufe von Kriminellen oder aufgrund eines Warnhinweises auf dem PC.

Anrufe von Microsoft oder Apple

Der Betrug beginnt damit, dass Opfer von angeblichen Microsoft-Service-MitarbeiterInnen oder Microsoft-Service-Mitarbeitern, selten auch von Apple-Mitarbeiterinnen oder Apple-Mitarbeitern angerufen werden. In gebrochenem Deutsch oder Englisch wird der oder die Angerufene dann auf einen Virus, einen Trojaner oder ein ähnliches Computerproblem hingewiesen. In weiterer Folge rät die freundliche Person am Telefon dazu, das Problem sofort zu beheben und erklärt auch genau, wie das funktioniert. Da es jedoch recht schwierig ist das Problem zu lösen, bietet die Anruferin bzw. der Anrufer Hilfe an.

Watchlist Internet: Anruf von Microsoft? – Legen Sie sofort auf!

Gefälschte Warnhinweise auf dem PC

Oftmals tappen Opfer auch aufgrund von gefälschten Warnhinweisen (Pop-ups) auf dem Computerbildschirm in diese Betrugsfalle. Die betrügerischen Warnhinweise poppen beispielsweise beim Surfen im Internet plötzlich auf und weisen auf ein dringliches Problem hin. Die Betroffenen werden aufgefordert, beim Fake-Service-Dienst anzurufen.

Eine vermeintliche Problembehebung mit Folgen

Erkennt das Opfer den Betrug nicht und kommt den Anweisungen der angeblichen Service-Mitarbeiterinnen oder Service-Mitarbeitern nach, muss ein Programm installiert werden, genauer gesagt eine Fernwartungssoftware. Damit können die vermeintlichen Service-Mitarbeiterinnen und -Mitarbeiter auf den Computer zugreifen und die Klicks der Opfer genau verfolgen. Haben die Kriminellen nun Zugriff auf den Computer, richten sie enormen Schaden an, indem sie zum Beispiel Schadsoftware installieren, Daten löschen oder stehlen. Weiters versuchen die Kriminellen an unterschiedliche Zugangsdaten (z. B. Amazon, Kreditkartendaten oder Onlinebanking-Daten) zu kommen. Mit dem Vorwand die Funktionsfähigkeit dieser Websites zu testen, werden Opfer aufgefordert sich wie gewohnt einzuloggen. Im Hintergrund werden jedoch heimlich Benutzername und Passwort erspäht. In weiterer Folge werden die Opfer sogar aufgefordert, für die vermeintliche Problembehebung zu bezahlen!

Call-ID-Spoofing

Das Tückische an betrügerischen Microsoft-Anrufen ist, dass in vielen Fällen auf dem Handybildschirm keine unbekannte Nummer, sondern ein eingehender Anruf von „Microsoft“ angezeigt wird. Das ist möglich, weil Kriminelle die Rufnummernübermittlung mittels einer illegalen Technologie namens Call-ID-Spoofing manipulieren und die wahre Rufnummer durch eine bestimmte Bezeichnung (z. B. einen Firmennamen) oder eine andere Rufnummer ersetzen.

Wie kann ich mich vor Tech-Support-Scams schützen?

- Pop-ups nicht blind vertrauen und keinesfalls Telefonnummern anrufen oder unbekannte Links anklicken.
- Unerwartete Anrufe von angeblichen Service-Mitarbeiterinnen und -Mitarbeitern bekannter Unternehmen nicht annehmen oder gleich auflegen. Denn: Microsoft oder Apple rufen in keinem Fall persönlich an.
- Keine unbekannten Programme installieren und Fremden keinesfalls den uneingeschränkten Zugriff auf den Computer ermöglichen.

Was können Opfer tun?

- Programme, die auf Anraten der Kriminellen installiert wurden, umgehend deinstallieren.
- Das System kann mit dem Windows Defender oder – falls vorhanden – mit einem Virenprogramm auf Schadsoftware überprüft werden.
- Um den Schaden zu beheben, muss meist das System neu aufgesetzt werden.
- Opfer sollten alle Passwörter ändern.
- Wurde für den vermeintlichen Service bezahlt, können Opfer versuchen, eine Rückholung der Überweisung zu bewirken oder auf eine Kulanzlösung des Kreditkarteninstitutes hoffen.
- Opfer sollten den Betrug bzw. den Betrugsversuch zur Anzeige bringen.
- Tech-Support-Scams können auch direkt an Microsoft gemeldet werden.

SCHADSOFTWARE

Wie der Begriff „Schadsoftware“ nahelegt, handelt es sich dabei um Software, die das Ziel verfolgt, jemandem zu schaden bzw. etwas zu beschädigen. Wie diese Schadsoftware – oft auch als „Malware“ bezeichnet – schädigt, ist jedoch von der Art der Software abhängig. Bekannte Arten sind beispielsweise Ransomware, die Systeme verschlüsselt, Spyware, die Systeme ausspioniert oder Viren, die zerstören Daten und sich selbstständig weiterverbreiten. Als Eingangstor dient Kriminellen insbesondere das Social Engineering, bei dem Menschen manipuliert und zur Installation von Schadsoftware gebracht werden. Auch Supply-Chain-Angriffe, Drive-By-Downloads und Software-Exploits werden genützt, Malware auf Zielsysteme zu installieren.

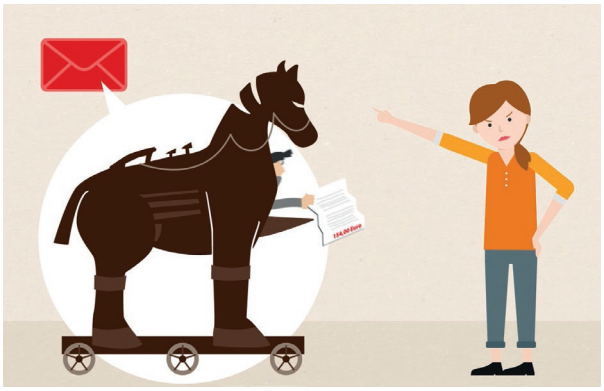


Abb. 14: Trojaner

Wie wird Schadsoftware auf Computersysteme installiert?

Es gibt unterschiedliche Methoden, wie Systeme mit Schadsoftware infiziert werden können. Auf das Social Engineering und Drive-by-Downloads wird hier genauer eingegangen. Die Themen „Supply-Chain-Angriffe“ und „Software-Exploits“ werden in gesonderten Kapiteln näher beschrieben.

Social Engineering

Kriminelle setzen dabei beispielsweise auf die „Sicherheitslücke Mensch“ indem sie Social Engineering betreiben. Das heißt, dass sie Personen dazu bringen, Daten bekanntzugeben, Schadsoftware selbst auf ihren Systemen zu installieren oder den Kriminellen zumindest Zugang zu einem System zu ermöglichen, sodass diese anschließend Angriffe starten können. Die Kriminellen setzen hierbei keine technischen Hacks ein, bei denen sie Software manipulieren oder Sicherheitslücken in Programmen ausnützen, die Hacks finden auf psychologischer Ebene statt.

Ein klassisches Beispiel für das Social Engineering sind Phishing-Mails im Namen bekannter Unternehmen. Die Betrügerinnen und Betrüger hinter den Nachrichten erschleichen sich dabei das Vertrauen ihrer Opfer, indem sie sich zum Beispiel als bekannte Bank ausgeben. Je glaubhafter der Inhalt und das Design der Nachricht, desto höher ist die Wahrscheinlichkeit, dass die adressierte Person die abgefragten sensiblen Daten bekanntgibt bzw. den Anweisungen zur Installation vermeintlicher Sicherheitssoftware folgt. Werden derartige E-Mails in personalisierter Form verschickt, spricht man von Spear-Phishing. Die Kriminellen nützen dabei Social Media oder Unternehmens-Websites als Informationsquelle zu ihrer Zielperson.

Eine weitere Art des Social Engineerings ist das sogenannte „Baiting“. Hierbei wird ein „Bait“ – also ein physischer Köder – ausgelegt. Dieser Köder kann beispielsweise ein USB-Stick oder eine CD mit Schadsoftware sein, die auf dem Arbeitsplatz der Zielperson oder einfach im Bürogebäude des Zielunternehmens platziert wird. Die Hackerinnen und Hacker erhoffen sich dadurch, dass jemand den entsprechenden Datenträger findet und die Schadsoftware auf dem eigenen PC installiert. Die Folge wäre eine unmittelbare Installation von Schadsoftware auf dem betroffenen Gerät oder gar auf dem gesamten Netzwerk.

Der Grund für diese Art des Angriffs ist meist der geringere Aufwand im Vergleich zum Eindringen über Lücken in Sicherheitssoftware. Wie folgendes Beispiel zeigt, kann auch auf diese Weise großer Schaden erzeugt werden: 2013 gelang es Kriminellen, die Kreditkartendaten von 40 Millionen Target-Kundinnen und -Kunden zu stehlen, indem sie über Social Engineering Zugriff auf das Netzwerk eines Zulieferers von Target ergatterten. Dieser Zugriff erlaubte in weiterer Folge Einsicht in das Netzwerk von Target selbst und ermöglichte das Auslesen sämtlicher Kreditkarteninformationen.

Drive-by-Downloads

Wie der Name bereits nahelegt, beschreiben Drive-by-Downloads das Herunterladen von Software „im Vorbeifahren“. Das Vorbeifahren beschreibt dabei den Aufruf einer Website. Diese Website löst beim Laden einen Download von schädlicher Software im Hintergrund aus, ohne dass die betroffene Person davon etwas mitbekommt. Die Kriminellen nützen dafür Sicherheitslücken in Browsern oder entsprechenden Plugins, wie Java oder Adobe Flash Player, aus. Ohne eine solche Sicherheitslücke ist kein Drive-By-Download möglich, was die Bedeutung der rechtzeitigen Installation von Sicherheitsupdates zeigt.

Exploits

Verständlich erklärt: Stellen Sie sich vor, Sie leben in einem Haus, bei dem ein Fenster nicht richtig eingebaut wurde. Dieses schlecht eingebaute Fenster stellt eine „Sicherheitslücke“ dar, denn ein Einbrecher könnte so mit einer Brechstange („Exploit“) die Schwachstelle ausnutzen und in Ihr Haus eindringen, um wertvolle Gegenstände zu stehlen. Ähnlich funktioniert auch ein sogenannter Exploit. Dabei handelt es sich also nicht um die Schadsoftware selbst, sondern um das Werkzeug (die Brechstange). Erst durch dieses Werkzeug erhalten Kriminelle Zugang zu Ihrem System (das Haus) und können Ihnen so Schaden zufügen (Diebstahl).

Bei Exploits handelt es sich um kleine Programme, die Sicherheitslücken auf einem Computer suchen und diese „ausnutzen“ („to exploit“). Wurden Sicherheitslücken gefunden, speichern die Angreiferinnen bzw. Angreifer einen schädlichen Code auf dem Computer. Meist wird dann erst in einem späteren Schritt die eigentliche Schadsoftware nachgeladen. Bei einem solchen Nachladen der Schadsoftware spricht man auch von einem „Payload“.

Wer ist betroffen?

Exploits sind eine sehr weit verbreitete Art der Internetkriminalität. Sie richten sich meist an große Digitalkonzerne, wie zum Beispiel Google, Apple, Microsoft, Adobe, WordPress oder Mozilla. Dadurch kann rein theoretisch jedes Unternehmen und jede Person, die diese Programme verwendet, Opfer von einem Angriff mittels Exploit werden.

Ob und bei wem die Schadsoftware tatsächlich nachgeladen wird, hängt jedoch von der Absicht der Angreiferinnen und Angreifer ab. So gibt es auch „gutartige“ Exploits, bei denen es lediglich darum geht, Unternehmen auf Schwachstellen in ihrer Software hinzuweisen. Oft werden Exploits auch benutzt, um Industriespionage zu betreiben. Davon sind nicht nur Unternehmen mit wachsendem Erfolg betroffen, sondern auch kleinere Unternehmen, die in besonders umkämpften Branchen tätig sind.

Es kann aber auch sein, dass mithilfe eines Exploits Schadsoftware bei möglichst vielen Nutzerinnen und Nutzern und dadurch auch bei Einzelpersonen eingeschleust werden soll. Manchmal laden die Kriminellen gar nicht selbst die Schadsoftware hoch, sondern verkaufen den Exploit auf dem Schwarzmarkt.

Seit 2014 führt Google eine Liste mit, bekannt gewordenen Exploits. Über diesen Link ist die Liste einsehbar: https://googleprojectzero.blogspot.com

Unter https://www.exploitalert.com kann außerdem nach betroffenen Internet-Anwendungen und Programmen gesucht werden.

Wie gehen die Angreiferinnen und Angreifer vor?

Wie die Angreiferinnen und Angreifer bei einem Exploit vorgehen, hängt davon ab, um welche Art von Exploit es sich handelt. Weit verbreitet sind Exploits, die sich durch das Surfen im Internet auf dem Computer verbreiten, sowie Exploits, die sich in Dateien verstecken und per Mail versendet werden. Insgesamt kann zwischen folgenden fünf Arten unterschieden werden:

- **Remote Exploits/Drive-by-Download:** Die Betroffenen surfen im Internet und im „Vorbeigehen“ („drive-by“) wird ein Exploit heruntergeladen. Die Opfer merken davon nichts. Solche Exploits können sich zum Beispiel in Werbebannern auf Websites verstecken – oftmals sogar auf seriösen und vertrauenswürdigen Websites. Klicken Sie auf den Werbebanner, wird im Hintergrund der Download gestartet. Dabei handelt es sich meist und „Exploit Kits“, also eine Sammlung von Exploits, die in verschiedenen Programmen (zum Beispiel in Browsern wie Firefox oder in PDF-Readern) nach Sicherheitslücken suchen.
- **Lokaler Exploit durch Öffnen von Dateien:** Bei Exploits, die sich in Dateien verstecken, ist ein gezielterer Angriff möglich. Dieser richtet sich meist an Unternehmen, denen E-Mails mit schädlichen Datei-Anhängen geschickt werden. Die Datei kann dabei aussehen wie eine Rechnung oder auch wie eine Bewerbung. Tatsächlich handelt es sich aber um Exploits, die nach dem Öffnen Sicherheitslücken im betroffenen Programm (zum Beispiel Microsoft Word oder Adobe Acrobat Reader) suchen.
- **Denial-of-Service-Exploits** (auch DoS-Exploit): Bei Denial-of-Service-Exploits wird kein schädlicher Programmcode ausgeführt, sondern versucht eine Anwendung zu überlasten. Diese Überlastung führt dazu, dass Dienste nicht mehr funktionieren. Dadurch können konkurrierende Unternehmen geschädigt oder Unternehmen erpresst werden.
- **Command-Execution-Exploits:** Die Angreiferinnen oder Angreifer steuern einen Programmcode, der über weitreichende Rechte über das System verfügt. Diese Art von Exploit ist besonders gefährlich, da die Kriminellen dabei Rechte erlangen, mit denen großer Schaden angerichtet werden kann.
- **SQL-Injection-Exploits:** Für Webanwendungen, die auf sogenannte SQL-Datenbanken zurückgreifen, können SQL-Injection-Exploits verwendet werden. Diese Datenbankabfragen werden dabei manipuliert. Die

Kriminellen können beispielsweise auf einer Login-Seite die dort eingegeben Daten so verändern, dass sie sich in einen eigentlich ungültigen Account einloggen können.

Nachdem die Angreiferinnen und Angereifer erfolgreich eine geeignete Sicherheitslücke gefunden haben, folgen die nächsten Schritte:

- Es wird ein schädlicher Code abgelegt.
- Der Programmfluss wird umgeleitet, damit der schädliche Code ausgeführt wird.
- Sobald der eingeschleuste Code aktiv ist, kann der Exploit Informationen über das System sammeln oder weitere schädliche Codes nachladen.
- Erst zum Schluss wird die eigentliche Schadsoftware geladen.

Gut zu wissen: Eine wichtige Funktionsweise von Exploits ist es, dass sie den Programmfluss umleiten. Um dies zu verstehen, ist es wichtig zu wissen, wie ein Programm überhaupt funktioniert: Wird ein Programm ausgeführt, finden nacheinander viele kleine Prozesse statt. Ein Prozessschritt hängt dabei immer vom vorangegangenen Schritt ab. Wie die Abfolge dieser einzelnen Schritte abläuft, wird im Code des Programms festgelegt. Exploits verändern diese Abfolge und lenken den Programmfluss direkt auf den schädlichen Code.

Wie unterscheidet sich ein Zero-Day-Exploit von einem herkömmlichen Exploit?

Wird eine Software entwickelt, werden viele Zeilen Code geschrieben. Dieser Programmcode wird immer komplexer, daher können beim Programmieren einer Software durchaus Fehler passieren und so Sicherheitslücken entstehen. Wenn das Unternehmen, das eine bestimmte Software programmiert hat, von solchen Sicherheitslücken erfährt, veröffentlicht es in der Regel eine „geflickte" Version („Patch") davon. Die Nutzerinnen und Nutzer können diese aktualisierte Version dann herunterladen.

Doch es ist nicht immer der Fall, dass die Unternehmen die Schwachstellen schnell bemerken und dagegen vorgehen können. Zero-Day-Exploits zielen auf unbekannte Sicherheitslücken ab, durch die die Kriminellen ins System eindringen können. Das betroffene Unternehmen hat dadurch null Tage (zero days) Zeit, um einen Schaden abzuwehren, denn in der Regel haben die Angreiferinnen und Angreifer die Sicherheitslücke schon lange zuvor entdeckt und Schadsoftware eingeschleust.

BEISPIEL APPLE MAIL

Im April 2020 machte das US-amerikanische Unternehmen ZecOps einen Zero-Day-Exploit im Programm Apple Mail bekannt. Die Sicherheitslücke soll mindestens seit 2012 bestehen, aktiv ausgenutzt wird die Sicherheitslücke seit Januar 2018. Betroffen sind Nutzerinnen und Nutzer eines iPhones oder eines iPads, die auf ihren Geräten ein Betriebssystem ab der Version iOS 6 verwenden.
Die Angreiferinnen und Angreifer verschicken dabei Mails, durch die der schädliche Code eingeschleust wird. Diese müssen teilweise nicht einmal geöffnet werden, damit der Angriff erfolgreich ist. Das Laden des schädlichen Codes ermöglicht den Kriminellen, E-Mails zu verändern, zu löschen und zu veröffentlichen. Die Opfer selbst merken nichts vom Angriff, auch weil von den Kriminellen verschickte Mails wieder gelöscht werden und daher nicht sichtbar sind. Laut ZecOps gab es jedoch mehrere Angriffe, beispielsweise auf Mitarbeiterinnen und Mitarbeiter von US-amerikanischen Unternehmen, auf einen Journalisten in Europa und auf eine prominente Person in Deutschland.
Bericht von ZecOps: https://blog.zecops.com/vulnerabilities/youve-got-0-click-mail/

Wie schützt man sich vor Exploits?

Mit folgenden Maßnahmen können sich Unternehmen und Einzelpersonen vor Exploits schützen:

- Updates, Updates, Updates! Egal, ob Computer, Laptop oder Handy: Das eigene Gerät regelmäßig zu aktualisieren, ist die wichtigste und wirksamste Maßnahme, wenn es um Internetsicherheit geht. Wird ein Programm auf den neuesten Stand gebracht, werden auch die aktuellen Patches mitinstalliert. Dadurch werden bekannte Sicherheitslücken geschlossen und das Gerät wird sicherer.
- Informiert man sich immer wieder über bekannt gewordene Sicherheitslücken, kann man potenziellen Schäden aktiv entgegenwirken, indem man auf Alternativprogramme zurückgreift. Im Falle des Apple Mail Exploits wurde beispielsweise empfohlen andere Mail-Programme auf dem iPhone oder iPad zu verwenden.
- Anti-Viren-Programme können Angriffsmuster erkennen und davor warnen. Gleiches gilt für Firewalls, die vor allem bei Exploits im Internet Alarm schlagen können.

Zero-Day-Exploits werden durch Anti-Viren-Programme oder Firewalls nicht erkannt. Einzelpersonen können das Ausnutzen von unbekannten Sicherheitslücken nicht verhindern. Vielmehr sind hier die Unternehmen

gefragt, damit Programme sorgfältig auf Schwachstellen und Programmierfehler geprüft werden.

Weiterführende Links:

https://www.watchlist-internet.at/schadsoftware/

https://www.watchlist-internet.at/news/kriminelle-versuchen-durch-serioese-programme-schadsoftware-zu-verbreiten/

Supply-Chain-Angriffe

Verständlich erklärt: Stellen Sie sich vor, Sie haben einen Kuchen bei einer Konditorei in Auftrag gegeben. Der Kuchen ist fertig, Sie gehen in die Konditorei und sind zufrieden, denn er sieht aus wie immer. Der Konditor bietet Ihnen aber noch ein „Update" mit Kirschen an. Sie stimmen zu und können den „aktualisierten" Kuchen morgen abholen. Doch bevor der Konditor die Kirschen auf dem Kuchen platzieren kann, schleichen sich Betrügerinnen und Betrüger in die Konditorei und infizieren die Kirschen mit einem Wurm. Der Konditor bekommt davon nichts mit, nutzt die infizierten Kirschen, um Ihren Kuchen „upzudaten" und verkauft ihn an Sie. Auch Sie bemerken nichts vom Wurm, außer dass Sie Bauchschmerzen nach dem Verzehr des Kuchens bekommen. So ungefähr lässt sich eine „Supply-Chain-Attacke" beschreiben.

Bei Supply-Chain-Angriffen wird an eine Vielzahl von Opfern Schadsoftware über eine vermeintlich vertrauenswürdige Quelle verteilt. Bei dieser neuen Art der Bedrohung werden Unternehmen nicht direkt angegriffen, sondern über ihre Lieferketten („supply chains"). Bekannte und seriöse Programme, Dienste und auch Hardware werden von den Kriminellen kompromittiert, also mit Schadsoftware infiziert. Diese Attacken stellen eine große Gefahr dar, da es sein kann, dass ein seit Jahren genutztes Programm plötzlich schädlich ist. Dadurch sind Angriffe über die Lieferketten auch nur schwer erkennbar.

Wer ist betroffen?

Supply-Chain-Angriffe sind vor allem für Unternehmen gefährlich. Laut einer Studie des Versicherers Hiscox aus dem Jahr 2019 waren 65 Prozent der befragten Unternehmen von einem solchen Angriff betroffen. Auch wenn sich kleinere Unternehmen oftmals für zu unbedeutend halten, um von Cyberkriminellen fokussiert zu werden, waren 2019 bereits 47 Prozent der Klein- und 36 Prozent der mittelständischen Betriebe Opfer verschiedener Cyberattacken. Insbesondere bei Supply-Chain-Angriffen können die Kriminellen – durch die Attacke einer einzigen Firma – zahlreiche Unternehmen treffen.

Eine Studie des Sicherheitsanbieters Sophos zeigt gleichzeitig, dass Supply-Chain-Angriffe von IT-Managerinnen und -Managern noch stark unterschätzt werden: Lediglich 16 Prozent der Befragten schätzen solche Angriffe als Bedrohung für die IT-Sicherheit ein.

Hiscox-Cyber-Readiness-Report 2019:
https://www.hiscox.de/wp-content/uploads/2019/04/Hiscox-Cyber-Readiness-Report-2019.pdf

The Impossible Puzzle of Cybersecurity:
https://secure2.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-impossible-puzzle-of-cybersecurity-wp.pdf

Wie gehen die Angreiferinnen und Angreifer vor?

Die meisten Menschen vertrauen Softwareherstellerinnen und -herstellern, wenn diese eine App, ein Programm oder ein anderes Produkt aktualisieren oder ein neues Produkt auf den Markt bringen. Doch genau dieses Vertrauen nutzen Kriminelle aus. Sie suchen nach dem anfälligsten Teil einer Lieferkette, um dort einzudringen und die Anwendungen mit Schadsoftware zu infizieren. So gelangt die Schadsoftware durch eine vertrauenswürdige Quelle an zahlreiche Nutzerinnen und Nutzer.

Dabei gibt es verschiedene Möglichkeiten, welchen Teil der Lieferkette die Kriminellen nutzen, um in eine Anwendung einzudringen und dort den Schadcode hinzuzufügen:

- In Entwicklungsumgebungen oder Update-Infrastrukturen von Software-Unternehmen wird nach Sicherheitslücken gesucht und die Schadsoftware darin versteckt. Gibt es dann ein neues Release einer Software oder ein Sicherheitsupdate wird die Schadsoftware über offizielle Vertriebskanäle verbreitet.
- Anwendungen werden – noch bevor sie signiert und damit offiziell vertrieben werden dürfen – mit Schadsoftware infiziert. Durch gestohlene Zertifikate oder mithilfe der Identität der Entwicklerinnen und Entwicklern werden die infizierten Anwendungen signiert und können dadurch verbreitet werden.
- Verwendet ein Software-Unternehmen Komponenten von Drittanbietern, kann auch in diese Komponenten ein infizierter Code eingeschleust werden. Der bösartige Code kann sich so auf Tausenden von Programmen ausbreiten.
- Die Schadsoftware wird auf den physischen Geräten (z. B. auf Smartphones, Tablets, USB-Sticks, Kameras) vorinstalliert.

Bevor die Software oder auch die physischen Geräte überhaupt kompromittiert werden können, brauchen die Kriminellen einen Zugang. Meist starten die Angriffsversuche daher mit sogenannten Spear-Phishing-Attacken, also mit zielgerichteten E-Mails, durch die versucht wird an vertrauliche Daten zu kommen. Auch Social-Engineering-Methoden sind beliebt, durch diese versuchen die Angreiferinnen und Angreifer das Verhalten von Personen so zu manipulieren, dass sie zum Beispiel vertrauliche Informationen preisgeben.

Sowohl die Phishing-Mails als auch das Social Engineering richten sich an Mitarbeiterinnen und Mitarbeiter des betroffenen Unternehmens, die möglichst hohe Netzwerkprivilegien haben. Haben die Kriminellen erste Informationen erhalten, versuchen sie immer weiter in das Unternehmensnetzwerk vorzudringen. Schon bei diesem Prozess werden Schwachstellen im Netzwerk genutzt, um weitere Anmeldeinformationen zu erhalten, bis sie schließlich Zugang zu den kritischen Systemen haben, in denen sie ihre Schadsoftware installieren können.

BEISPIEL CCLEANER

Einer der bekanntesten Supply-Chain-Angriffe war jener auf die CCleaner-Software. Die Software dient dazu das Windows-Betriebssystem zu optimieren und ist nicht nur bei Unternehmen, sondern auch bei Privatnutzerinnen und -nutzern äußerst beliebt. Kriminelle konnten in die Entwicklungsumgebung eindringen und dort ihren schädlichen Code installieren.

CCleaner ist ein Beispiel, das zeigt, wie komplex Attacken auf die Lieferketten sein können. Im August 2017 wurde die neue, verseuchte Version von CCleaner veröffentlicht. Nicht nur bis zur Veröffentlichung, sondern auch ein Monat danach blieb der bösartige Code unerkannt. Dadurch stand das schädliche Programm einen Monat lang zum Download zur Verfügung. Der CCleaner-Hersteller Piriform schätzt, dass 1,7 Millionen Computer infiziert wurden.

Doch nicht alle waren von der tatsächlichen Schadsoftware betroffen, denn die erste Virusstufe sammelte lediglich Daten der betroffenen Geräte, um herauszufinden, ob diese für die Kriminellen überhaupt interessant sind. Mit der Schadsoftware wurden in einer zweiten Stufe hauptsächlich Telekommunikations- und Technikunternehmen infiziert, vor allem in Japan, Taiwan, Deutschland und den USA (z. B. Sony, Samsung, Asus oder Fujitsu).

Wie schützt man sich vor Supply-Chain-Angriffen?

Einige Sicherheitsforscher und Sicherheitsforscherinnen sind davon überzeugt, dass es viele Softwareprogramme gibt, die aufgrund von Supply-Chain-Chain-Attacken kompromittiert, aber bisher noch nicht entdeckt wurden. Um diesen Trend zu stoppen, sind die Softwareentwicklerinnen und Softwareentwickler gefragt, bessere interne Revisionen und starke Code-Review-Praktiken einzuführen, bevor ein Produkt für Verbraucherinnen und Verbraucher freigegeben wird. Zudem sollten alle Produkte eine digitale Signatur besitzen und nur über sichere und verschlüsselte Kanäle verteilt werden. Im Allgemeinen haben Unternehmen auch einen besseren Zugang zu starken Sicherheitslösungen und Technologien als Konsumenten.

Dennoch können auch Unternehmerinnen und Unternehmer und private Nutzerinnen und Nutzer das Risiko eines Supply-Chain-Angriffes verringern: Unternehmen sollten die Sicherheitskompetenz ihrer Mitarbeiterinnen und Mitarbeiter laufend stärken. Einen gewissen Grad an Sicherheitskompetenz müssen aber auch private Anwenderinnen und Anwender besitzen, um die verschiedenen Gefahren zu erkennen. Dadurch kann beispielsweise verhindert werden, dass Dienste oder Programme verwendet werden, bei denen bekannt ist, dass sie für das Verteilen von Schadsoftware missbraucht werden. Auch ungewöhnliches Verhalten von bestimmten Programmen oder Diensten kann so rascher erkannt werden.

Weiterführende Links:

https://www.watchlist-internet.at/schadsoftware/

https://www.watchlist-internet.at/news/kriminelle-versuchen-durch-serioese-programme-schadsoftware-zu-verbreiten/

Welche Arten der Schadsoftware gibt es?

Der Begriff Schadsoftware beschreibt sämtliche Computerprogramme bzw. Codes, die den Zweck verfolgen Schaden zuzufügen. Wie der Schaden zugefügt wird, ist dabei völlig offen. Genauer betrachtet werden anschließend Ransomware, Spyware, Viren und Trojaner. Daneben gibt es weitere Arten von Schadsoftware, die aber keine derart bedeutende Rolle spielen oder Mischformen und leichte Abwandlungen darstellen.

Ransomware

Ransomware stellt mittlerweile eine der größten Gefahren für Unternehmen und Privatpersonen dar, wenn es um Schadsoftware geht. Es handelt sich dabei um eine bösartige Software, die eine Verschlüsselung des betroffenen Systems vornimmt und somit den Zugriff auf

sämtliche Dateien verhindert. Der Name ergibt sich aus dem darauffolgenden Vorgehen der Kriminellen. Nach der Verschlüsselung des jeweiligen Systems taucht auf dem Bildschirm ein entsprechender Hinweis auf die vorgenommene Verschlüsselung auf und die weitere Nutzung des Systems ist fortan unmöglich. Die einzige Möglichkeit, die Verschlüsselung aufzuheben, ist die Zahlung eines Lösegelds (Ransom = Lösegeld). Der häufigste Weg für die Installation von Ransomware ist das Social Engineering. Die Software ist meist in gefährlichen E-Mail-Anhängen oder Chatnachrichten enthalten, die nichtsahnend geöffnet werden und die Verschlüsselung unmittelbar auslösen. Auch Drive-by-Downloads können Ransomware enthalten.

Die Geldforderungen der Kriminellen hinter den Angriffen unterscheiden sich je nach Ziel. Bei Privatpersonen bewegen sie sich meist im drei- bis vierstelligen Bereich. Bei großen Konzernen betragen die Forderungen hingegen oft mehrere Millionen Euro. Von einer Zahlung der Forderungen ist aber dringend abzuraten. Einerseits ist nicht sicher, ob die Dateien sich durch eine Zahlung tatsächlich wieder freischalten lassen, andererseits ist nicht auszuschließen, dass nicht weitere Schadsoftware eingeschleust wurde, die im Hintergrund weiterläuft und beispielsweise Zugriff auf sensible Dateien ermöglicht.

Der einzig effektive Schutz vor Ransomware ist die Vorsicht beim Öffnen von Dateien oder Ausführen von Programmen sowie das Anlegen von Backups, sodass sämtliche Daten im Falle eines Angriffes wiederherstellbar sind.

Spyware

Spyware beschreibt eine Art von Software, die Computer oder andere Geräte, die sich mit dem Internet verbinden, ausspioniert. Alle Daten, die das schädliche Programm auslesen kann, werden an die Kriminellen weitergegeben und können für weitere Verbrechen genützt oder verkauft werden. Die gesammelten Infos reichen von Interessen, besuchten Websites oder Online-Einkäufen bis hin zu Passwörtern, Login-Daten sowie Kreditkarten- und Onlinebanking-Informationen. Auch Spyware landet häufig über Social Engineering auf Systemen. Oft ist sie aber auch Teil sogenannter Freeware, also Gratis-Software. So kann die Installation eines kostenlosen File-Sharing-Programms verdeckt auch zur Überwachung des betroffenen Systems führen. Vorsicht ist hier auch bei Nutzungsvereinbarungen geboten, denn häufig wird zur Nutzung grundsätzlich seriöser Dienste und Anwendungen vorausgesetzt, dass man Datenweitergaben zustimmt, die kaum von den Weitergaben bei Spyware zu unterscheiden sind.

Es gibt unterschiedliche Arten von Spyware. Einige sind darauf ausgelegt möglichst viele Informationen und gespeicherte Daten abzugreifen. Betroffene Systeme werden dabei gescannt und es wird alles gespeichert, was gefunden wird.

Eine häufig genutzte Sonderform von Spyware sind sogenannte Keylogger. Diese zeichnen bei Hardware-basierten Lösungen jeden einzelnen Tastendruck auf oder fertigen bei Software-basierten Lösungen Screenshots in passenden Momenten an. In beiden Fällen wird den Verantwortlichen das Auslesen sensibler Eingaben ermöglicht.

Andere Formen sind beispielsweise Password Stealers, die insbesondere auf das Auslesen von Passwörtern spezialisiert sind, sowie Banking-Trojaner, die sich gegen Bankinstitute richten und mitunter Transaktionswerte ändern können.

Trojaner

Trojaner sind meist als seriöse Programme getarnte Schadsoftwares, die über eine Hintertür das Auslesen von oder den Fremdzugriff auf betroffene Systeme zulassen. Der Name ist dabei in Anlehnung an das Trojanische Pferd entstanden. Auch Trojaner gelangen durch Social Engineering, Freeware-Programme, Drive-by-Downloads oder unseriöse Anhänge und Chatnachrichten auf die Zielsysteme. Die Funktionsweisen der verschiedenen Trojaner unterscheiden sich stark. Sie werden häufig als Viren bezeichnet, können sich aber nicht wie Viren selbst ausführen oder vermehren, weshalb diese Bezeichnung nicht korrekt ist.

Sogenannte Backdoor-Trojaner eröffnen eine Art Hintertür, die es Kriminellen je nach Komplexität des Trojaners erlaubt, Datenverkehr auszulesen oder sogar Veränderungen auf dem System aus der Ferne durchzuführen. Dadurch wäre beispielweise die Installation weiterer Schadsoftware möglich.

Eine andere Form – Download-Trojaner – erlaubt es den Kriminellen nicht, direkt über eine Hintertür Veränderungen vorzunehmen. Stattdessen löst die Installation weitere Downloads aus. Diese enthalten meist noch mehr Schadsoftware.

Banking-Trojaner sind mit der steigenden Beliebtheit von Onlinebanking-Diensten aufgekommen. Sie ermöglichen es den Kriminellen beispielsweise, die betroffenen User beim Aufruf des Onlinebankings auf gefälschte Onlinebanking-Websites weiterzuleiten. Diese sehen den echten zum Verwechseln ähnlich, eingegebene Daten landen aber bei den Kriminellen statt bei den Banken.

DDoS-Trojaner werden für DDoS-Attacken genützt. DDoS steht dabei für „Distributed Denial of Service“ und kann als mutwillige Dienstblockade durch Überlastung be-

zeichnet werden. Die Trojaner erfüllen dabei den Zweck, dass infizierte Systeme von Kriminellen dafür verwendet werden können, andere Systeme zu überlasten. Soll beispielsweise eine Website überlastet werden, werden alle infizierten Systeme dazu genützt, diese Website aufzurufen und so die Server zu überlasten. Dies führt in weiterer Folge dazu, dass die Website für die Dauer des Angriffs nicht mehr erreichbar ist.

Viren

Computerviren sind Programme, die sich selbst weiterverbreiten und sich in andere Programme oder auch Hardware einschleusen. Die Bezeichnung „Viren" entstand also in Anlehnung an biologische Viren, die sich ebenso vermehren können und passende Wirtszellen befallen. Wie andere Schadsoftwares verfolgen Viren das Ziel, Schaden zu verursachen. Dies tun sie beispielsweise, indem sie Systemdateien beschädigen, Ressourcen verschwenden oder Daten zerstören. Das Stehlen oder Verschlüsseln von Daten hingegen ist meist keine Funktion der Viren. Das größte Unterscheidungsmerkmal zu anderer Schadsoftware ist aber, dass sie sich ohne Zustimmung des Betroffenen selbst replizieren oder auf andere Systeme verbreiten können.

Viele Computerviren entstehen oder entstanden als eine Art Scherz und – anders als biologische Viren – ausschließlich durch Menschenhand. Bei harmlosen Varianten können die Konsequenzen einer Infektion noch als lustig angesehen werden. So kursierte lange Zeit ein Virus, der bei Aktivierung zu einem ständigen Öffnen und Schließen des CD-Laufwerks führte und relativ leicht wieder zu entfernen war. Ein anderer Virus änderte beispielsweise sämtliche betroffenen Dateien in Bilder von Tintenfischen, was im ersten Moment lustig klingen mag, tatsächlich aber bereits zu erheblichem Schaden führen konnte. Aggressivere Formen von Computerviren sind sogar in der Lage Hardware zu zerstören oder Systeme und Programme soweit zu überlasten, dass sie nicht mehr benutzbar sind.

Was schützt effektiv vor Schadsoftware?

Einen hundertprozentigen Schutz vor Schadsoftware gibt es leider nicht. Ein guter Verhaltensgrundsatz ist aber: „Erst denken, dann klicken".

- Programme aus unbekannten Quellen sollten vermieden werden: Pop-up-Fenster, die zur Installation von Software auffordern, müssen ignoriert werden. Stattdessen sollten Downloads von den offiziellen Websites der jeweiligen Programme erfolgen.
- Datei-Anhänge in E-Mails und Chatnachrichten dürfen nur mit größter Vorsicht geöffnet werden: Ist nicht klar, wer die E-Mail abgeschickt hat, Ungereimtheiten auftauchen oder Grund zur Unsicherheit besteht, sollten Anhänge nicht geöffnet werden.
- Betriebssystem und Programme müssen immer auf dem aktuellen Stand gehalten werden: Die laufende Installation von Updates schützt am besten vor Sicherheitslücken.
- Eine Trennung von Administrator- und Benutzerkonten ist ratsam: Im (Arbeits-)Alltag sollte ausschließlich das Benutzerkonto verwendet werden. Bei der Installation von Software wird immer das Administrator-Passwort abgefragt. Die unbemerkte Installation von Software im Hintergrund wird dadurch erheblich erschwert.
- Interne oder externe Firewall- und Anti-Viren-Programme aktivieren und nützen: Die meisten Betriebssysteme bieten mittlerweile gute integrierte Schutzmaßnahmen, weshalb oft keine zusätzliche Software notwendig ist. Am wichtigsten ist es, sowohl integrierte als auch etwaige zusätzliche Schutzmaßnahmen zu aktivieren und auf dem aktuellen Stand zu halten.
- Es sollten immer umfangreiche Backups angelegt werden: Im Falle von Schadsoftware-Angriffen ist so jederzeit die Wiederherstellung von Daten möglich und ein großer Teil der Schäden kann schnell wieder behoben werden.

Wurde ein System bereits mit Schadsoftware infiziert, muss diese vom System entfernt werden. Dafür kann eine vollständige Neuinstallation des Systems notwendig sein. Im Falle diverser Viren kann auch das zu wenig sein, wodurch die Hardware womöglich ersetzt werden muss. Bei einer Verschlüsselung des Systems sollte ebenfalls auf Backups und eine Neuinstallation gesetzt werden. Von der Bezahlung erpresster Geldbeträge ist abzusehen. Wenn der Verdacht naheliegt, dass Zugriff auf sensible Daten durch Fremde möglich war, sollten umgehend sämtliche Zugangsdaten geändert werden, die womöglich betroffen sind. Auch die Kontaktaufnahme zur Bank ist meistens empfehlenswert. Zu guter Letzt sollte Anzeige erstattet werden, wenn Schäden entstanden sind oder sensible Daten gestohlen werden konnten.

Weiterführende Links:

https://www.watchlist-internet.at/news/detail/News/so-schuetzen-sie-sich-effektiv-vor-schadsoftware/

https://www.watchlist-internet.at/news/detail/News/wofuer-schadsoftware-genutzt-werden-kann/

https://www.watchlist-internet.at/news/unternehmen-aufgepasst-versand-gefaehrlicher-mails-im-namen-des-bundeskanzleramts/

https://www.watchlist-internet.at/news/schadsoftware-in-vermeintlichen-banking-apps-aus-unbekannter-quelle/

SICHERE PASSWÖRTER

Sichere Passwörter schützen nicht nur vor den Zugriff Fremder auf private Informationen, sie schützen vor allem vor finanziellem Schaden und Identitätsmissbrauch. Daher ist auf die Passwort-Sicherheit besonderen Wert zu legen.

Passwörter sind wie der Schlüssel zum eigenen Haus oder der eigenen Wohnung. Wer den Schlüssel hat, hat freien Zutritt in meine ganz privaten Räume und kann anschauen und mitnehmen, was beliebt.

Im Internet ist der private E-Mail-Account einer der privatesten Räume. Zwar findet die Kommunikation inzwischen nur noch selten per E-Mail statt, vieles läuft aber noch immer im E-Mail-Postfach zusammen. Hier sind Informationen zu gebuchten Reisen ebenso zu finden wie getätigte Online-Einkäufe und Rechnungen für Internet, Handy, Strom usw. Wer Zutritt zum E-Mail-Postfach hat, kann also herausfinden, was man alles nutzt und kann sich oft sogar Zutritt dazu verschaffen. Die E-Mail-Adresse ist nämlich meistens der Weg, über den sich Passwörter zurücksetzen lassen. Haben Kriminelle erst einmal Zutritt zu meinen Online-Konten, nutzen sie diese, um z. B. in meinem Namen und auf meine Kosten einzukaufen oder in meinem Namen betrügerische Nachrichten zu versenden.

Beim Schutz der eigenen Nutzerkonten im Internet geht es also nicht allein darum, Privates vor Fremden zu verbergen, es geht vor allem darum, finanziellen Schaden und Identitätsmissbrauch zu verhindern. Ein wichtiger Baustein ist dabei ein sicheres Passwort.

Zum Thema „Sicheres Passwort“ gibt es zahlreiche Tipps, doch welche davon sind sinnvoll?

- Lange Passwörter verwenden
- Passwörter nicht mehrfach verwenden
- Passwörter regelmäßig ändern
- Passwortgenerator verwenden
- Ziffern, Sonderzeichen sowie Groß- und Kleinbuchstaben verwenden
- Passwörter nicht notieren
- Zwei-Faktor-Authentifizierung verwenden

Lange Passwörter verwenden

„Je länger, desto besser“ ist eine der wichtigsten Passwort-Regeln. Ein Passwort mit 8 Zeichen, das mit einer weit verbreiteten Verschlüsselungsmethode in der Datenbank eines Nutzerkontos gespeichert ist, lässt sich derzeit in 6 Minuten errechnen. Für ein Passwort mit 10 Zeichen sind es aktuell 5 Wochen. Gelangt eine solche Datenbank in die Hände von Kriminellen, können sie die Nutzerkonten, die mit einem kurzen Passwort geschützt sind, also leicht übernehmen, bei einem langen Passwort ist dies kaum möglich. Mit einem 16 Zeichen langen Passwort ist man derzeit gut gesichert.

Passwörter nicht mehrfach verwenden

Haben Kriminelle Zugriff auf die Zugangsdaten einer Internetseite, probieren sie aus, bei welchen anderen Internetseiten die Zugangsdaten auch funktionieren. Verwendet man dasselbe Passwort also für mehrere Nutzerkonten, ist es sehr wahrscheinlich, dass alle Konten übernommen werden. Daher ist es sinnvoll, jedes Passwort nur einmal zu verwenden.

Passwörter regelmäßig ändern

Durch das regelmäßige Ändern von Passwörtern werden alte Passwörter, die in die Hände von Kriminellen gelangen, wertlos. Müssen Passwörter zu oft geändert werden, besteht allerdings die Gefahr, dass die Passwortsicherheit darunter leidet. Aus „Instagram1238“ wird dann oft „Instagram1239“. Solche neuen Passwörter lassen sich leicht erraten. Passwörter müssen immer dann geändert werden, wenn ein Datenhack einer Seite bekannt wird. Ansonsten ist es nicht notwendig, ein sicheres Passwort regelmäßig zu ändern.

Bei Diensten wie Have I been pwned (https://haveibeenpwned.com) oder dem HPI Identity Leak Checker (https://sec.hpi.de/ilc/search) lässt sich überprüfen, von welchen Seiten Datenhacks bekannt sind.

Passwortgenerator verwenden

Selbst ausgedachte Passwörter lassen sich viel einfacher knacken als maschinell generierte. Dabei ist es egal, wie komplex das selbst erdachte Passwort ist.
(Mehr dazu: https://www.spiegel.de/netzwelt/web/passwoerter-warum-selbst-ausgedachte-kennwoerter-oft-unsicher-sind-a-1282751.html)

Zur Erstellung von sicheren Passwörtern sollten unbedingt Passwortgeneratoren verwendet werden. Passwortgeneratoren wie jener der Uni Münster (https://www.uni-muenster.de/IT-Sicherheit/passwortgenerator.html), von Passwortsafes (z. B. LastPass) (https://www.lastpass.com/de/password-generator) oder 1Password (https://1password.com/de/password-generator/) gelten als sicher. Generell muss aber darauf geachtet werden, wer den Passwortgenerator anbietet: Die erstellten Passwörter könnten nämlich heimlich gespeichert werden.

Ziffern, Sonderzeichen sowie Groß- und Kleinbuchstaben verwenden

Je komplizierter ein Passwort ist, desto schwieriger ist es zu erraten. Groß- und Kleinbuchstaben sowie Ziffern sind daher ein Muss für ein sicheres Passwort. Sonder-

zeichen sollten auch verwendet werden, sind aber nicht überall zulässig.

Passwörter nicht notieren

Wer alle bisher genannten Tipps für ein sicheres Passwort berücksichtigt, wird sich kein einziges Passwort merken können. Sichere Passwörter kann man sich nicht merken!

Daher ist es notwendig, Passwörter zu notieren. Eine handgeschriebene Liste, die zu Hause an einem sicheren Ort verwahrt wird, ist zwar ziemlich sicher, aber unpraktisch: Ein zufällig generiertes und 16 Zeichen langes Passwort lässt sich schwer abtippen. Einfacher wäre es, die Passwörter aus einem Textdokument zu kopieren, das auf dem Computer gespeichert ist. Das ist allerdings unsicher und absolut nicht empfehlenswert.

Die derzeit sicherste und gleichzeitig komfortabelste Variante sind Passwort-Safes wie zum Beispiel: Keepass (https://keepass.info/), LastPass (https://www.lastpass.com/de) oder 1Password (https://1password.com/de/). In Passwort-Safes werden Passwörter verschlüsselt gespeichert. Die benötigten Passwörter müssen entweder herauskopiert werden oder werden von einem Browser-Plugin automatisch ausgefüllt. In der Basis-Version sind die Programme meist kostenlos, weitere Funktionen, wie z. B. die Nutzung auf Smartphones, kosten ein paar Euro im Monat. Zur Verwaltung von Passwörtern sind Passwort-Safes derzeit die sicherste und empfehlenswerteste Möglichkeit.

Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (auch: Zwei-Schritte- oder Zwei-Wege-Authentifizierung) ist eine zusätzliche Sicherheitsmaßnahme zum Schutz von Benutzerkonten: Zusätzlich zum Passwort muss beim Login eine weitere Sicherheitskomponente eingeben werden, z. B. ein PIN-Code. Dieser Code wird etwa auf die im Nutzerkonto hinterlegte Handynummer gesendet oder es kommt ein Code-Generator zum Einsatz (z. B. Microsoft Authenticator). Selbst wenn Passwörter in die falschen Hände gelangen, haben Unbefugte auf diese Weise keinen Zugriff auf das Benutzerkonto.

Ein sicheres Passwort …

… ist also mindestens 16 Zeichen lang, wird nur für ein Nutzerkonto verwendet, wurde mit einem sicheren Passwortgenerator erstellt, enthält Groß- und Kleinbuchstaben, Ziffern und nach Möglichkeit auch Sonderzeichen, wird in einem Passwortsafe gespeichert und in regelmäßigen Abständen geändert.

Darüber hinaus gibt es Passwort-Strategien, die Passwörter zwar weniger sicher, dafür leichter merkbar machen:

- „4-Wörter-Methode“:
  Aus vier zufälligen Wörtern wird ein komplexes und sehr langes Passwort zusammengesetzt und durch ein Sonderzeichen getrennt. Zum Beispiel „Babybrei$Einhorn$Thomas$Semmel“. Dadurch entsteht ein sehr langes zufälliges Passwort, das recht einfach zu merken ist.
- Zeichen schlagen Wörter:
  Die Sonderzeichen können auch mit Zahlen ergänzt werden. Zum Beispiel „Babybrei&Einhorn2Thomas%-Semmel1!“.

Weiterführende Links:

Saferinternet.at: Wie sieht ein sicheres Passwort aus?
https://www.saferinternet.at/faq/datenschutz/wie-sieht-ein-sicheres-passwort-aus/

Saferinternet.at: Wie kann ich Passwörter sicher aufbewahren?
https://www.saferinternet.at/faq/datenschutz/wie-kann-ich-passwoerter-sicher-aufbewahren/

Saferinternet.at: Warum unterschiedliche Passwörter verwenden?
https://www.saferinternet.at/faq/datenschutz/warum-sollte-ich-unterschiedliche-passwoerter-verwenden

Saferinternet.at: Was ist die Zwei-Faktor-Authentifizierung?
https://www.saferinternet.at/faq/datenschutz/was-ist-die-zwei-faktor-authentifizierung/

SICHERES ONLINESHOPPING

Hinter Onlineshops können auch Kriminelle stecken, die Konsumentinnen und Konsumenten das Geld aus der Tasche ziehen sowie persönliche Daten und Kreditkar-tendaten stehlen wollen. Für ein positives Einkaufser-lebnis ohne böse Überraschungen sollten Konsumen-tinnen und Konsumenten wissen, wie seriöse Webshops aussehen und woran sie betrügerische Onlineshops er-kennen.

Fake-Shops und Markenfälscher

Grundsätzlich wird im Onlinehandel zwischen zwei be-trügerischen Modellen unterschieden: Fake-Shops und Markenfälscher-Shops.

Fake-Shops sind betrügerische Onlineshops, die eine Zahlung mittels Vorauskasse verlangen, die bestellte Ware jedoch nicht liefern. Fake-Shops sind meist sehr professionell und ansprechend aufgebaut, haben voll-

ständige Impressumsangaben und wirken insgesamt sehr vertrauensvoll. In Wahrheit wurden sämtliche Angaben jedoch frei erfunden oder von anderen Unternehmen gestohlen. Fake-Shops sind häufig erst bei genauerem Hinsehen als Betrug erkennbar.

Markenfälscher-Shops bieten meist gefälschte Markenprodukte und Designer-Kleidung zu Spottpreisen an bzw. wird das gesamte Sortiment stark vergünstigt beworben. Opfer erhalten in der Regel sogar Produkte, jedoch von minderwertiger Qualität – oder ein Produkt, das nicht bestellt wurde. Die meisten Markenfälscher-Shops sind sehr unprofessionell umgesetzt, was die Erkennung erleichtert.

Einen Fake-Shop erkennen

- Preis: Der Preis des Produktes ist billiger als bei anderen Anbieterinnen und Anbietern. Meist sind aber nur bestimmte Produkte im Angebot, andere werden zu den üblichen Preisen angeboten.
- Zahlungsmöglichkeiten: Die Ware kann nur per Vorkasse bezahlt werden.
- Fehlermeldungen: Beim Check-out kann manchmal auch Kreditkartenzahlung oder PayPal gewählt werden. Wählt man diese, kommt es jedoch zu einer Fehlermeldung, dass die gewünschte Zahlungsmethode aufgrund von technischen Schwierigkeiten gerade nicht verfügbar sei.
- Widersprüchliche Angaben: In den Geschäftsbedingungen werden Zahlungsmethoden angeführt, die beim Check-out nicht verfügbar sind.
- Internetrecherche: Eine kurze Recherche zum Shop kann sehr aufschlussreich sein, denn häufig wird bereits vor betrügerischen Shops gewarnt.
- Impressum: Die Impressumsdaten sind frei erfunden oder wurden von einem seriösen Unternehmen gestohlen.
- Gütezeichenmissbrauch: Um möglichst vertrauenswürdig zu wirken, missbrauchen die Kriminellen Gütezeichen, die einen sicheren Onlineshop auszeichnen.

Watchlist Internet: Zahlreiche Fake-Shops locken mit günstigen Pools, Griller & Terrassenmöbel
Watchlist Internet: Vorsicht beim E-Bike-Kauf: Fake-Shop ebike-quadrat.com bietet günstige E-Bikes an!

Markenfälschungen erkennen

- Preis: Teure Markenprodukte werden stark vergünstigt angeboten. In der Regel wird das gesamte Sortiment zu „Spottpreisen“ angeboten.
- Unplausible Webadresse: Markenfälscher-Shops haben meist seltsame Webadressen, die nicht wirklich zum Angebot passen. So werden beispielsweise teure Markenschuhe unter der Domain „freiwillige-feuerwehr-bad-kleinen.de“ verkauft. Und: Endet eine Shop-Adresse auf .at oder .de hat dies nicht zu bedeuten, dass der Shop von Österreich oder Deutschland aus betrieben wird.
- Währungsauswahl: Markenfälscher-Shops haben sehr häufig eine Währungsauswahl.
- Fehler: Markenfälscher-Shops weisen häufig sprachliche Fehler auf, beispielsweise wird der Menüpunkt „Rückgaberecht“ sehr häufig als „Kehrt zurück“ bezeichnet. Markenfälscher-Shops erkennt man auch an wechselnden Sprachen und schlechter Übersetzung.
- Fehlendes Impressum: Auf der Website findet sich kein oder nur ein unvollständiges Impressum.
- Fehlende Kontaktangaben: Auf der Website finden sich keine Kontaktangaben bzw. nur ein kurzes Onlineformular für Anfragen. Oftmals stammen die angeführten E-Mail-Adressen von kostenlosen Anbietern wie Hotmail oder Gmail.
- Unvollständige Geschäftsbedingungen: Die Geschäftsbedingungen sind kurz, unvollständig, schlecht übersetzt oder mit irrelevanten Inhalten befüllt.
- Unsichere Verbindung: Markenfälscher-Shops haben meist keine sichere Verbindung. Eine solche erkennt man am Schloss vor der Webadresse.

Watchlist Internet: Vorsicht bei (zu) günstiger Markenware im Internet!
Watchlist Internet: ludwig-therese.net ist Fake

Tipps zur Überprüfung eines Onlineshops

- Den Onlineshop mit dem Zusatz „Fake“ oder „Erfahrungen“ im Internet suchen. Oftmals wird vor dem betrügerischen Shop bereits gewarnt. Vorsicht: Werden keine relevanten Suchergebnisse angezeigt, ist das meist auch ein Hinweis auf einen betrügerischen Onlineshop.
- Der gängige Marktpreis eines Produktes kann mittels Vergleichsplattformen wie geizhals.at oder idealo.at recherchiert werden.
- Die „Liste betrügerischer Online-Shops“ checken. Möglicherweise wurde der Shop bereits von der Watchlist Internet als betrügerisch eingestuft.
- Die rechtmäßige Verwendung von Gütezeichen kann überprüft werden.
- Auch die Richtigkeit von Impressumsangaben kann mit ein wenig Recherche überprüft werden.

Exkurs: Gütezeichen überprüfen

Damit echte Onlineshops seriöse Gütezeichen auf ihren Websites darstellen dürfen, müssen sie strenge Prüfverfahren durchlaufen und gewisse Kriterien erfüllen. Betrügerische Onlineshops versuchen daher häufig, über gefälschte oder erfundene Zertifikate und Gütezeichen Vertrauen zu stiften. Bei seriösen Gütezeichen wie dem Österreichischen E-Commerce-Gütezeichen, Trusted Shops oder Trustmark Austria können Konsumentinnen

und Konsumenten daher durch einen Klick auf das Gütezeichen-Logo ganz einfach überprüfen, ob es sich um ein echtes Zertifikat handelt. Sollte kein Klick auf ein Gütezeichen möglich sein oder eine Verlinkung ins Leere führen, kann der Shop auch im Register der Zertifikatsstellen gesucht werden, z. B. unter www.guetezeichen.at/zertifizierte-websites. Gibt es dort keinen Hinweis auf die Echtheit eines Gütezeichens, so ist Vorsicht geboten. Bei der Recherche ist auch darauf zu achten, dass man tatsächlich auf der Seite der jeweiligen Zertifikatsstellen landet und nicht auf einer gefälschten Seite, die ebenso von den Kriminellen eingerichtet wurde.

Exkurs: Impressumsdaten überprüfen

In der Regel können Fake-Shops bereits anhand des Preises, der Zahlungsmethode und der Erfahrungen im Internet entlarvt werden. Kann aufgrund dessen noch keine Einschätzung getroffen werden, kann in einem weiteren Schritt die Richtigkeit der Impressumsdaten kontrolliert werden.

- Die UID-Nummer kann im „MwSt.-Informationsaustauschsystem (MIAS)“ unter https://ec.europa.eu/taxation_customs/vies/?locale=de überprüft werden. Ist die Nummer ungültig, kann von Fake ausgegangen werden. Achtung: Ist die UID-Nummer gültig, bedeutet das nicht unbedingt, dass der Shop seriös ist. Kriminelle stehlen meist die UID-Nummer eines bestehenden Unternehmens. Um mehr über die Herkunft der UID-Nummer herauszufinden, kann diese beispielsweise auch im Internet gesucht werden.
- Die angeführte Firmenadresse kann in einem Online-Kartendienst gesucht werden. Erscheint der Firmensitz unplausibel (z. B. in einer Wohngegend oder einem Wohnhaus) kann Betrug nicht ausgeschlossen werden.
- Der Firmenname kann in einer Firmendatenbank gesucht werden (Deutschland: handelsregister.de, Österreich: firmen.wko.at, europaweit: e-justice.europa.eu/content_find_a_company-489-de.do?clang=de).
- Konsumentinnen und Konsumentenkönnen unter whois.com feststellen, wer eine Webadresse wann registriert hat. Finden sich keine eindeutigen Angaben dazu oder besteht der Shop erst seit Kurzem, weist dies meist auf Betrug hin.

Hilfe, ich habe in einem betrügerischen Shop bestellt

- Es besteht zwar ein gesetzliches Rücktrittsrecht, allerdings ist dieses bei betrügerischen Unternehmen mit Sitz außerhalb der EU kaum durchsetzbar. Trotzdem können Opfer versuchen, Kontakt zum Unternehmen aufzunehmen.
- Sofern man kein Retouren-Label erhält, ist ein Rückversand der Ware nicht empfehlenswert. Es ist nämlich unwahrscheinlich, dass die bezahlten Beträge und Portokosten rückerstattet werden.
- Wurde per Kreditkarte bezahlt, können sich Opfer mit dem Kreditkartenanbieter in Verbindung setzen und die Geschehnisse schildern. Möglicherweise kann eine Rückbuchung des Betrages veranlasst werden. Darauf besteht zwar kein Rechtsanspruch, doch häufig ergibt sich eine Kulanzlösung.
- Achten Sie bei einer Kreditkartenzahlung auf ungerechtfertigte Abbuchungen, denn Kriminelle haben durch die Bestellung möglicherweise Zugriff auf diese erlangt. Gemäß § 67 ZaDiG 2018 sind Beträge, die ohne die Zustimmung der Inhaberin bzw. des Inhabers abgebucht wurden, vom Zahlungsdienstleister zurückzuerstatten!
- Wurde per PayPal bezahlt, können Opfer versuchen, das Geld über den Käuferschutz zurückzubekommen.
- Kommt es zu keiner Rückbuchung bezahlter Beträge, sollten Opfer Betrugsanzeige bei der Polizei erstatten.
- Wurde vorab bezahlt, ist das Geld höchstwahrscheinlich verloren. Opfer können sich an die Bank wenden, die Erfolgschancen für eine Rückholung sind jedoch gering.
- Bei Fragen können sich Opfer an die Watchlist Internet wenden und betrügerische Shops melden.

SMART HOME

„Smart Home“ soll das Wohnen angenehmer machen. Hinter dem Begriff verbergen sich digitale Anwendungen, die einem Aufgaben im Haushalt abnehmen bzw. vereinfachen. Auch die Sicherheit des Haushalts kann dadurch erhöht werden. Setzt man allerdings auf falsche Geräte, öffnet man Kriminellen Tür und Tor.

Dass der Kühlschrank selbständig die Einkäufe erledigt, ist noch Zukunftsmusik und wirft die Frage auf, ob man das wirklich will. In den Bereichen Beleuchtung, Heizung, Sicherheit oder Sprachsteuerung sind digitale Lösungen aber bereits in die Haushalte vorgedrungen. Richtig angewendet machen sie das Leben etwas leichter.

Wer seiner Heizung z. B. eine digitale Steuerung verpasst, die per App bedient werden kann, kann die Heizung rechtzeitig vor dem Heimkommen aus dem Urlaub einschalten und muss sie nicht durchgehend laufen lassen oder erst einmal frieren, wenn die Heizung abgeschaltet war. Das spart Heizkosten und macht das Heimkommen angenehmer. Aber auch im Alltag hilft eine gezielte Heizungssteuerung dabei, Kosten zu sparen.

Durch die LED-Technologie sind für die Beleuchtung der eigenen vier Wände zahlreiche neue Möglichkeiten dazugekommen. Deutlich kleinere Lampen oder Lichtschläuche ermöglichen es beispielsweise, indirektes Licht an Stellen einzusetzen, an denen es vorher nicht möglich war. So lässt sich die Atmosphäre im Raum jederzeit anpassen. Mit aktuellen, digital gesteuerten Be-

leuchtungssystemen lässt sich das Licht aber nicht nur ein- und ausschalten oder dimmen. Lampen lassen sich z. B. auch einzeln schalten oder die Lichttemperatur (der Weißton) lässt sich anpassen: Für die Hausarbeit ein motivierendes, kaltweißes Licht, für den gemütlichen Abend im Wohnzimmer ein heimeliges, warmweißes Licht. Durch voreingestellte Schaltprogramme lässt sich auch bei Abwesenheit simulieren, dass jemand zu Hause ist und eine App-Steuerung ermöglicht, das Licht einzuschalten, bevor man nach Hause kommt. Das unangenehme Heimkommen in die dunkle Wohnung gehört damit der Vergangenheit an. Türschlösser, Sprechanlagen und Videoüberwachung sind weitere Sicherheitsanwendungen, die sich digital steuern lassen.

Alle gängigen Systeme lassen sich mit einer Sprachsteuerung verbinden. So lässt sich das Licht nicht nur per Schalter oder App steuern, auch mit einem Sprachbefehl vom Wohnzimmersofa aus kann man das Licht ein- und ausschalten.

Der große Vorteil dieser digitalen Lösungen liegt darin, dass sie individuell an die eigenen Bedürfnisse angepasst werden können. Neben den Funktionen sollte bei der Auswahl einer „Smart-Home"-Lösung aber auch auf die Sicherheit geachtet werden.

Schutz vor unbefugtem Zugriff

Mit einem klassischen Lichtschalter wird der Strom ein- oder ausgeschaltet. Fließt Strom, leuchtet die Lampe. Bei einer digitalen Lösung ist der Strom immer eingeschaltet. Mit Schalter oder App wird der Lampe direkt mitgeteilt, ob und wie hell sie leuchten soll. Schalter/App und Lampe kommunizieren also miteinander. Damit das Licht, die Heizung oder auch der Türöffner nicht von Fremden gesteuert werden kann, muss diese Kommunikation möglichst gut gegen Zugriffe von Unbefugten abgesichert werden. Die Herstellerfirmen arbeiten dabei mit unterschiedlichen Strategien, die mehr oder weniger sicher sind.

Jedes Gerät ist direkt mit dem Internet verbunden

Die unsicherste Variante ist, wenn mit jedem verwendeten Gerät einen direkten Zugang zum Internet hergestellt wird. Meistens sind diese Geräte über das WLAN mit dem Internet verbunden. Die Steuerung erfolgt also über das Internet. Vor allem bei günstigen Überwachungskameras oder Spielzeugen wird diese Variante eingesetzt.

Leider überwiegen die Nachteile: Die Verbindung zum Internet ist nicht geschützt und kann auch nicht konfiguriert werden. Fällt das Internet aus, funktioniert das Gerät nicht. Nicht nur man selbst kann die eigenen vier Wände überwachen, auch Kriminelle können sehen, was vor der Kamera oder im Kinderzimmer passiert.

Ein Steuerungsgerät stellt die Verbindung zum Internet her

Ein Steuerungsgerät ist die Schaltzentrale: Von dort aus werden alle verbundenen Geräte gesteuert. Schaltet man mithilfe eines Lichtschalters das Licht ein, geht der Schaltbefehl zuerst an das Steuerungsgerät und von dort an die Lampe. Alle Konfigurationen sind im Steuerungsgerät gespeichert, die verbundenen Geräte kommunizieren über Kabel oder über eine verschlüsselte Funkverbindung. Dadurch ist das Ganze ein geschlossenes System, in das Kriminelle, wenn überhaupt, nur mit sehr großem Aufwand eindringen können.

Das Steuerungsgerät lässt sich mit dem Internet verbinden. Das Ermöglicht die Steuerung von unterwegs per App. Im Gegensatz zu Einzelgeräten, die mit dem Internet verbunden werden, gibt es bei dieser Variante nur ein Gerät, das direkt mit dem Internet verbunden ist. Das minimiert die Angriffsstellen für Kriminelle. Außerdem sind solche Steuerungsgeräte in der Regel deutlich besser gegen fremden Zugriff geschützt, als es Einzelgeräte sein können. Innerhalb der Wohnung funktioniert das System auch, wenn das Internet ausfällt. Lediglich die Steuerung von außen ist dann nicht mehr möglich.

Die Qual der Wahl

Bei der Auswahl der passenden Systeme muss immer eine Abwägung zwischen Sicherheit, Komfort und Funktion vorgenommen werden:

- Eine Überwachungskamera, bei der Fremde mitschauen können und die ausfällt, wenn das Internet unterbrochen ist, bietet wenig Schutz. Ist sie aber gut gegen unbefugte Zugriffe abgesichert und zeichnet weiter auf, wenn das Internet ausfällt, bietet sie Schutz, auch wenn die Live-Übertragung auf das Smartphone unterbrochen wird.
- Lassen sich Licht oder Heizung nicht mehr regeln, wenn das Internet ausfällt, wird es im Smart Home schnell ungemütlich. Fällt lediglich die Steuerung von unterwegs aus, sind die Folgen überschaubar.
- Bei Sprachassistenz-Systemen ist eine direkte Internetverbindung sinnvoll, da sie ja nicht nur zur Steuerung des Smart Homes eingesetzt werden. Fragen nach dem Wetter, Kochrezepten oder aktuellen Nachrichten können nur beantwortet werden, wenn eine Internetverbindung besteht. Fällt diese aus, lässt sich das Smart Home aber trotzdem noch bedienen.

Generell gilt für die Sicherheit des Smart Homes: Werden Geräte per Kabel mit dem Internet verbunden, ist es sicherer als per WLAN. Je weniger direkte Verbindungen zum Internet bestehen, desto weniger Angriffspunkte gibt es für Kriminelle. Bei einem System mit Steuerungsgerät und verschlüsselter Funkverbindung besteht nur

eine einzige direkte Verbindung zum Internet. Das macht diese Variante besonders sicher. Vor dem Kauf muss man sich aber erkundigen, was mit den Nutzungsdaten passiert, die über die Internetverbindung auch zum Hersteller gelangen können. Hat der Hersteller kein Interesse an den Daten oder werden sie zu Marketingzwecken ausgewertet und weiterverkauft?

Eines haben allerdings alle Systeme gemeinsam: Fällt der Strom aus, ist nichts mehr „smart“ im Haus.

Tipp: Die Zeitschrift „Das Haus“ hat 2019 einen Vergleich verbreiteter Systeme zusammengestellt, der einen guten Überblick bietet:
https://www.haus.de/smart-home/die-besten-smart-home-systeme-im-vergleich

TEIL II:

HANDBUCH ZUR UNTERRICHTSGESTALTUNG

Im zweiten Teil des Leitfadens werden anhand von ausgewählten Themen Vermittlungsszenarien, Tipps, Materialien und Übungen für den praktischen Unterricht vorgestellt.

EINFÜHRUNG

Ältere Menschen sind eine heterogene Zielgruppe. „Die Seniorinnen und Senioren" gibt es nicht. Unter ihnen finden wir technikaffine Menschen, aber auch Personen, die den neuen Technologien abwartend bis ablehnend gegenüberstehen.

Die Aufgabe von EDV-Trainerinnen und EDV-Trainern ist, ältere Menschen über neue Technologien zu informieren, zu motivieren und sie auf ihrem Weg in die digitale Welt zu begleiten.

Neben dem entsprechenden Fachwissen benötigen Trainerinnen und Trainer auch didaktische Fähigkeiten sowie Offenheit und Empathie gegenüber älteren Menschen. Respekt, Geduld und ein eigenes positives Altersbild sind wesentliche Voraussetzungen, um Inhalte nachhaltig und erfolgreich vermitteln zu können.

Empfehlungen:
- Heterogenität der Zielgruppe nutzen
- Geschlechterrollen reflektieren
- positives Bild des Alterns vermitteln
- Angst nehmen und Sicherheitsbedürfnis unterstützen
- Selbstvertrauen stärken
- Eigenständigkeit fördern
- Motivation nutzen
- Wunsch nach Beziehungen unterstützen
- Erleichterung des Alltags unterstützen
- Spaß und Leichtigkeit vermitteln
- einfache Sprache verwenden
- mit Widerständen richtig umgehen
- Dauer und Lerntempo beachten
- Lernbegleitung statt Frontalunterricht
- Angebot flexibel gestalten
- nachlassende Sehkraft berücksichtigen
- motorische Probleme berücksichtigen
- Kurzzeitgedächtnis stützen

Maßnahmen für Seniorinnen und Senioren in der digitalen Welt
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/studie_massnahmen_fuer_senorinnen_in_der_digitalen_welt.pdf

Didaktische Strategien für Internet-Kurse für Seniorinnen und Senioren
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Didaktische_Strategien_Internet_Senior_innen_Kurse.pdf

WIE SPRECHE ICH SICHERHEITSTHEMEN AN?

Für eine sichere Internetnutzung ist es wichtig, über mögliche Gefahren Bescheid zu wissen. Ihre Aufgabe als Trainerin oder Trainer ist es, Einsteigerinnen und Einsteigern die häufigsten Betrugsmaschen im Internet aufzuzeigen und gleichzeitig Ihren Teilnehmenden Hilfestellungen zu geben, wie sie diese erkennen können und wie sie sich und ihr Gerät schützen können.

Sicherheitsthemen sind ein Querschnittsthema, wenn es um die Nutzung von digitalen Medien geht. Sie sollten im Unterricht immer miteinfließen, ohne zu große Angst zu machen.

> Tipp: Schulen Sie Ihre Teilnehmenden laufend, indem Sie den sicheren Umgang bei allen Themen einfließen lassen. Zu viele Informationen auf einmal zu Betrug und Fallen im Internet können schnell verunsichern und im schlimmsten Fall zur einer Nicht-Nutzung des Internets führen.

DER AUFBAU MEINER UNTERRICHTSEINHEIT

Beginnen Sie mit einem Beispiel aus der bekannten, analogen Welt.

Wir sperren unsere Haustür zu, um Unbefugte oder Kriminelle nicht in unsere privaten Räume einzuladen. Wir sind misstrauisch, wenn teure Artikel auf der Straße angeboten werden. Wir glauben Flugblättern nicht, die uns große Gewinnsummen versprechen. Wir geben Personen, die wir nicht kennen, keine hohen Geldsummen usw.

Finden Sie Beispiele, die Sie in die digitale Welt übertragen und erklären Sie Ihren Teilnehmenden, wie Kriminelle vorgehen. Im nächsten Schritt zeigen Sie ihnen anhand von Beispielen, woran unterschiedliche Betrugsfallen zu erkennen sind.

Tipp: Verwenden Sie im Unterricht die Präsentation „Internetkriminalität“ und die Folien „Fake oder nicht Fake?“ oder steigen Sie mit einem Video ein. (https://www.digitaleseniorinnen.at/leistungen/schulungsmaterialien/)

Die **Präsentation „Internetkriminalität“** bietet Informationen und Fallbeispiele u. a. zu folgenden Themen:
- Betrügerischer Verkauf im Internet
- Schadsoftware
- Phishing
- Antworten und Hilfe

Die **Präsentation „Fake oder nicht Fake?“** bietet ausgesuchte Fallbeispiele zur Einschätzung von Betrugsfällen mit Auflösung am Ende.

Erklärvideos gibt es zu folgenden Themen:
- Abo-Fallen
- Abo-Fallen auf Datingseiten
- Kleinanzeigenbetrug
- Sextortion
- Fake-Shops
- Gefälschte Rechnungen

Achten Sie darauf, dass Sie keine abwertenden Bemerkungen machen, wie: „Da muss man schon sehr unwissend sein, wenn man diese Betrugsfalle nicht rechtzeitig erkennt.“ Es könnten Teilnehmende bereits in die eine oder andere Betrugsfalle getappt sein. Erzählen Sie Ihren Teilnehmenden, dass auch technikaffine und routinierte Internet-User immer wieder Betrugsmaschen zum Opfer fallen.

Stellen Sie Informationen zur Verfügung, wo Teilnehmende Hilfe finden, wenn doch mal etwas passiert ist.

Tipp: Teilen Sie Ihren Teilnehmenden die **Broschüre „Betrug im Internet: So schützen Sie sich!“** aus.

Die Broschüre „Betrug im Internet“ mit den wichtigsten Infos & Tipps zu Fake-Shops, Markenfälschungen, Schadsoftware, Phishing, Abo-Fallen und Kleinanzeigenbetrug kann in der Printversion über das Broschürenservice von Saferinternet bestellt werden.

Die Bestellung und der Versand erfolgen kostenlos und innerhalb Österreichs.
https://www.saferinternet.at/services/broschueren-service/

Allgemeine Tipps für die Vermittlung von digitalen Themen
- Stellen Sie den Nutzen für die Zielgruppe dar.
- Knüpfen Sie an der bekannten analogen Welt an.
- Verwenden Sie Beispiele aus dem Alltag.
- Vereinfachen Sie komplexe Systeme.
- Erklären Sie Begriffe in einfacher Sprache.
- Zeigen Sie Risiken auf, ohne Angst zu machen.
- Geben Sie Tipps für die sichere Internetnutzung.
- Führen Sie mit den Teilnehmenden praktische Übungen durch, sofern dies möglich ist.
- Stellen Sie übersichtliche und gut lesbare Schulungsunterlagen zur Verfügung.

SICHERHEITSTHEMEN IM UNTERRICHT

GERÄTESICHERHEIT

Tipps für die sichere Smartphone-Nutzung
- Halten Sie Ihre persönlichen Zugangsdaten (z. B. PIN, Passwort) geheim.
- Laden Sie Apps nur aus dem offiziellen App-Shop Ihres Anbieters herunter.
- Vermeiden Sie Onlinebanking in öffentlichen WLAN-Netzen.
- Notieren Sie sich die Seriennummer Ihres Smartphones (IMEI-Nummer), diese wird im Falle eines Diebstahls für die Anzeige bei der Polizei benötigt.
- Installieren Sie Updates umgehend.
- Aktivieren Sie Dienste wie WLAN, Bluetooth und GPS nur bei Bedarf.
- Sichern Sie regelmäßig Ihre Daten.

Handout: Smartphone sicher nutzen. So schützen Sie Ihr Smartphone.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/12_Smartphone_sicher_nutzen.pdf

Tipps für die sichere Nutzung von Apps
- Laden Sie Apps nur aus den offiziellen App-Shops herunter.
- Lesen Sie die Bewertungen der Apps und installieren Sie schlecht bewertete Apps nicht.
- Achten Sie auf In-App-Käufe und aktivieren Sie diese nur bei Bedarf.
- Kontrollieren Sie die Zugriffsberechtigungen von Apps.
- Löschen Sie nicht mehr verwendete Apps.

Handout: Die Welt der Apps. Nützliche Helfer.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Die_Welt_der_Apps.pdf

INFORMATIONEN AUS DEM INTERNET

Tipps zum kompetenten Bewerten von Informationen und Angeboten aus dem Internet

- Seien Sie skeptisch.
- Überprüfen Sie die Quellen.
- Verwenden Sie Hoax-Datenbanken, um bekannte Falschmeldungen zu identifizieren. (www.mimikama.at, www.hoaxmap.org)
- Überprüfen Sie mit umgekehrter Bildsuche, ob ein Bild in einem anderen Zusammenhang verwendet wird (images.google.com, www.tineye.com)
- Informieren Sie sich auf der Website der Watchlist Internet über aktuelle Betrugsfallen.
- Installieren Sie die Watchlist-Internet-App (verfügbar für Android und iOS). (https://www.watchlist-internet.at/)

> Tipp: Installieren Sie im Rahmen einer Smartphone-Schulung gemeinsam diese kostenlose App der Watchlist Internet.

Handout: Wahr oder falsch? Informationen aus dem Internet bewerten.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Wahr_oder_falsch.pdf

EINKAUFEN IM INTERNET

Tipps für den sicheren Einkauf im Internet

- Informieren Sie sich vor dem Kauf über die Händlerin bzw. den Händler.
- Lesen Sie die Bewertungen des Shops.
- Lesen Sie die Produktbeschreibungen und „Kleingedrucktes" genau.
- Seien Sie misstrauisch bei auffällig günstigen Preisen oder „Gratisangeboten".
- Checken Sie, ob der Onlineshop auf der Watchlist-Internet-Website gelistet ist.
- Verwenden Sie eine sichere Bezahlmethode.

Handout: Online-Shopping. Aber sicher!
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Online-Shopping.pdf

BANKWEGE ONLINE ERLEDIGEN

Tipps für sicheres Onlinebanking

- Achten Sie darauf, dass auf Ihrem Gerät stets die aktuelle Version des Betriebssystems und des Browsers verwendet wird, Virenscanner und Firewalls installiert sowie Sicherheitsupdates vorgenommen wurden.
- Rufen Sie die Website Ihrer Bank durch Eintippen der Internetadresse in Ihrem Browser auf.
- Kontrollieren Sie, ob das Sicherheitsschloss im Browser geschlossen ist.
- Vermeiden Sie Onlinebanking in fremden oder öffentlichen WLAN-Netzen.
- Schützen Sie Ihre persönlichen Zugangsdaten und halten Sie diese geheim.
- Melden Sie sich immer ab (Logout).
- Klicken Sie keine Links in verdächtigen E-Mails an. Ihre Bank fordert Sie NIE per E-Mail oder telefonisch auf, Ihre Zugangsdaten oder vermeintliche Sicherheitscodes bekanntzugeben! Im Zweifelsfall kontaktieren Sie direkt Ihre Ansprechperson bei der Bank.

Handout: Online-Banking – Bankgeschäfte per Mausklick erledigen.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/10_Infoblatt_OnlineBanking_bf.pdf

PASSWÖRTER

Tipps für den sicheren Umgang mit Passwörtern

- Nutzen Sie für jedes Online-Konto ein anderes Passwort.
- Nutzen Sie einen Passwort-Manager für die Verwendung unterschiedlicher Passwörter.
- Ändern Sie Passwörter regelmäßig.
- Achten Sie bei der Eingabe des Passwortes darauf, dass Ihnen niemand über die Schulter sieht.
- Halten Sie Ihre Passwörter nicht auf einem Klebezettel am Monitor fest.

Ältere Menschen neigen häufig dazu, bei Passwörtern die eigenen Geburtsdaten, jene der Kinder bzw. Enkelkinder oder andere unsichere, leicht nachvollziehbare Kombinationen zu verwenden.

Machen Sie Ihren Teilnehmenden bewusst, dass Passwörter ähnlich wie Schlüssel für ihre Wohnungstür funktionieren und ihr digitales Eigentum und ihre Privatsphäre schützen.

Unterstützen Sie beim Erstellen schwer zu knackender Passwörter:

- Denken Sie sich einen für Sie einprägsamen Satz aus. Verwenden Sie die Anfangsbuchstaben.
  ***M**ein **F**ahrrad **s**teht **s**eit **O**ktober **2016** **i**n **d**er **G**arage.*
  → *MFssO2016idG*
- Überlegen Sie sich einen Satz, der nur für Sie eine Bedeutung hat.
  IchbinnochnieineinemrotenFerrarigefahren.

Für Fortgeschrittene bieten sich die Themen Passwort-Manager und Zwei-Faktor-Authentifizierung an.

Handout: Passwörter – die Schlüssel für Ihr digitales Zuhause
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/08_Infoblatt_Passwoerter_bf.pdf

PERSÖNLICHE DATEN SCHÜTZEN

Bei der Nutzung von digitalen Geräten und Online-Services werden unterschiedliche Daten zwischen Online-Diensten und Nutzerin bzw. Nutzer ausgetauscht. Wichtig ist daher, dass bewusst entschieden werden kann, wo wir welche Daten gegenüber wem bekanntgeben bzw. welche Daten durch die Verwendung digitaler Geräte bzw. verschiedener Programme (Apps) wo landen.

Geben Sie Ihren Teilnehmenden einen Überblick, fragen Sie nach verwendeten Apps und schauen Sie gemeinsam die vergebenen Zugriffsberechtigungen der Apps an.

Für die Einstellung der Privatsphäre in sozialen Netzwerken (Facebook, Facebook Messenger, Google, YouTube, WhatsApp, Instagram, Snapchat, TikTok) bietet Saferinternet Schritt-für-Schritt-Anleitungen:
https://www.saferinternet.at/privatsphaere-leitfaeden/

Machen Sie deutlich, wer welche Informationen eines Accounts (Kontos) sehen kann. (Privatsphäre-Einstellungen!) Siehe auch Privatsphäre-Leitfäden auf der Website von Saferinternet.at:
https://www.saferinternet.at/privatsphaere-leitfaeden

MATERIALIEN

INFOBLÄTTER

Phishing – Betrug im Internet.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Phishing.pdf

Die Welt der Apps. Nützliche Helfer.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Die_Welt_der_Apps.pdf

Online-Banking – Bankgeschäfte per Mausklick erledigen.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/10_Infoblatt_OnlineBanking_bf.pdf

Online-Shopping. Aber sicher!
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Online-Shopping.pdf

Passwörter – die Schlüssel für Ihr digitales Zuhause.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/08_Infoblatt_Passwoerter_bf.pdf

Smartphone sicher nutzen. So schützen Sie Ihr Smartphone.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/12_Smartphone_sicher_nutzen.pdf

Wahr oder falsch? Informationen aus dem Internet bewerten.
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Infoblatt_Wahr_oder_falsch.pdf

BROSCHÜREN

Betrug im Internet – so schützen Sie sich
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Flyer_Betrug_im_Internet.pdf

Passwörter – Informationen für Erwachsene in leicht lesbarer Sprache
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Passwoerter_Informationen_in_leichter_Sprache.pdf

Sicheres Bezahlen im Internet
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Sicheres_Bezahlen__im_Internet.pdf

Sicherheitseinstellungen für Smartphones (Android)
https://www.saferinternet.at/fileadmin/categorized/Materialien/ISPA_Sicherheitseinstellungen_Android_Phone.pdf

Sicherheitseinstellungen für Smartphones (iPhone)
https://www.saferinternet.at/fileadmin/categorized/Materialien/ISPA_Sicherheitseinstellungen_iOS_iPhone.pdf

Telefon, Handy & Internet: Rechnungskontrolle bringt's!
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Folder_info_telekomrechnung.pdf

PRÄSENTATIONEN

Präsentationsfolien: Betrug im Internet: Rechtzeitig erkennen und verhindern (PPTX)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Workshop_Betrug_im_Internet.pptx

Präsentationsfolien: Betrug im Internet: Rechtzeitig erkennen und verhindern (PDF)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Workshop_Betrug_im_Internet.pdf

Präsentationsfolien „Internetkriminalität“ (PPTX)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/PPT_Internetkriminalitaet.pptx

Präsentationsfolien „Internetkriminalität“ (PDF)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/PPT_Internetkriminalitaet.pdf

Präsentationsfolien „Fake oder nicht Fake?“ (PPTX)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/PPT_Fake_oder_nicht_Fake.pptx

Präsentationsfolien „Fake oder nicht Fake?“ (PDF)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/PPT_Fake_oder_nicht_Fake.pdf

Präsentationsfolien „Digitale Alltagskompetenzen“ (PPTX)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/PPT_Digitale_Alltagskompetenzen_vermitteln.pptx

Präsentationsfolien „Digitale Alltagskompetenzen“ (PDF)
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/PPT_Digitale_Alltagskompetenzen_vermitteln.pdf

VIDEOS

Abo-Fallen (Erklärvideo)
https://youtu.be/Xq16jkNa9Yc

Abo-Fallen auf Datingseiten (Erklärvideo)
https://youtu.be/ZUFTgFlfXzo

Fake-Shops im Internet (Erklärvideo)
https://youtu.be/PjoW5Cmim8k

Gefälschte Rechnungen (Erklärvideo)
https://youtu.be/UFt2M9Pz3M8

Kleinanzeigenbetrug (Erklärvideo)
https://youtu.be/XCq9QJ3oY38

Sextortion (Erklärvideo)
https://youtu.be/8EVUsMQhIPg

Sicheres Bezahlen im Internet (Video)
https://vimeo.com/328599936

LEITFÄDEN

Leitfaden für Trainerinnen und Trainer – Digitale Alltagskompetenzen vermitteln
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Leitfaden_Digitale_Alltagskompetenzen_vermitteln.pdf

Leitfaden für Trainerinnen und Trainer – Online-Schulungen planen und durchführen
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Leitfaden_Online_Schulungen.pdf

Leitfaden für Trainerinnen und Trainer ¬– Smart Speaker im praktischen Einsatz
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Leitfaden_Sprachassistenz_Systeme.pdf

STUNDENBILD

Zeit	Dauer	Inhalt	Übung	Vorbereitung
10:00	15 Min	Überblick	Begrüßung – Vorstellung der Inhalte	
10:15	30 Min	Präsentation Rätsel/Einschätzung	Fake erkennen?! Präsentation: „Fake oder nicht Fake?“ Anhand der Beispiele sollen TN einschätzen, ob es sich um Fake handelt oder nicht. Alle TN notieren still ihre Einschätzung, am Ende löst die/der TR die Beispiele.	Kopien der Notizzettel für alle Teilnehmenden austeilen (Vorlage in der Präsentation „Fake oder nicht Fake?“)
10:45	15 Min	Diskussion	Woran können Fakes erkannt werden? Sammeln von TN-Meldungen, auf Flipchart notieren	Flipchart
11:00	10 Min	Pause		
11:10	40 Min	Präsentation	Internetkriminalität – Betrugsfallen • Funktionsweise • Erkennungsmerkmale • Lösungswege und Hilfestellungen für Opfer	Präsentation „Internetkriminalität“ Ev. Erklärvideos Watchlist-Internet-App bei Bedarf
11:50	10 Min	FAQ	Offene Fragen beantworten	
12:00		Ende		

ANHANG

LINKLISTE

Bundesministerium für Inneres – Internetkriminalität
https://bundeskriminalamt.at/306/start.aspx

Bundesministerium für Inneres – Präventionstipps
https://bundeskriminalamt.at/202/Internet_kennen/start.aspx

Bundesministerium für Inneres – Folder: 5 Grundregeln im Internet
https://bundeskriminalamt.at/202/Internet_kennen/files/Internet_Folder_20200811.pdf

Cyber Security Quiz
https://ovosplay.com/de/cybersecurity-quiz/

Lagebericht Cybercrime 2018 – Entwicklungen, Phänomene und Schwerpunkte
https://bundeskriminalamt.at/306/files/Cybercrime_Report_18_web.pdf

Handy & Internet: Tipps rund um Telefonie, Online-Shopping & Apps
https://www.arbeiterkammer.at/beratung/konsument/HandyundInternet/index.html

Hilfe bei Rechtsproblemen mit Erotik-Portalen
https://datingfalle.at/

Internet Ombudsstelle – kostenlose Schlichtung und Beratung (Online-Shopping, Urheberrecht, Recht am eigenen Bild, Persönlichkeitsrechte etc.)
https://www.ombudsstelle.at/

Österreichisches E-Commerce-Gütezeichen
https://www.guetezeichen.at/

Privatsphäre-Leitfäden für soziale Netzwerke
https://www.saferinternet.at/privatsphaere-leitfaeden/

Saferinternet.at unterstützt vor allem Kinder, Jugendliche, Eltern und Lehrende beim sicheren, kompetenten und verantwortungsvollen Umgang mit digitalen Medien
https://www.saferinternet.at

Sicherheitseinstellungen für Smartphones (Android)
https://www.saferinternet.at/fileadmin/categorized/Materialien/ISPA_Sicherheitseinstellungen_Android_Phone.pdf

Sicherheitseinstellungen für Smartphones (iPhone)
https://www.saferinternet.at/fileadmin/categorized/Materialien/ISPA_Sicherheitseinstellungen_iOS_iPhone.pdf

Watchlist Internet ist eine unabhängige Informationsplattform zu Internet-Betrug und betrugsähnlichen Online-Fallen aus Österreich
https://www.watchlist-internet.at/

LESELISTE

Didaktische Strategien für Internet-Kurse für Seniorinnen und Senioren
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Didaktische_Strategien_Internet_Senior_innen_Kurse.pdf

Maßnahmen für Seniorinnen und Senioren in der digitalen Welt
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/studie_massnahmen_fuer_senorinnen_in_der_digitalen_welt.pdf

Methoden und Übungen in der Bildungsarbeit mit älteren Menschen
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/mobiseniora-teil-3-methoden-und-glossar.pdf

Themen in der Bildungsarbeit mit älteren Menschen
https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/mobiseniora-teil-2-themen-und-lebensbereiche.pdf

ÜBUNGEN

- 1. Dr. Google? – Gesundheitsinformationen aus dem Internet
- 2. Das gehört (nicht) online
- 3. Heiratsschwindel online
- 4. Meine Spuren im Netz
- 5. Was ich im Internet nicht sehen will

Titel der Übung	**1. „DR. GOOGLE?“ – GESUNDHEITSINFORMATIONEN AUS DEM INTERNET**
Ziele der Übung	Einen Überblick über gesundheitsrelevante Informationen bekommen. Seriosität von Angeboten einschätzen.
Setting	Einzelcoaching
Vorbereitung	Seriöse Seiten zu Gesundheitsfragen recherchieren und kennen (z. B. netdoktor.at).
Umsetzung	Zu aktuellen gesundheitlichen Fragen der TN wird gemeinsam überprüft, welche Quellen als seriös einzuordnen sind und warum. Als Kriterien zählen • die Seriosität der Autorinnen/Autoren, • die Finanzierung der Angebote und • die Aktualität der Angaben Dazu werden exemplarisch ausgewählte Seiten mit anderen verglichen, um sich einen Überblick zu verschaffen.
Zu beachten	Angebote und Quellen im Gesundheitsbereich ändern sich sehr rasch und sind in Bezug auf ihre Finanzierung oft schwer zu durchschauen. Dies sollte den TN vermittelt werden, ohne dabei Angst zu machen oder den Eindruck zu erwecken, dass alles im Internet falsch sei.
Unterlagen	Infoblatt: Wahr oder falsch? Informationen aus dem Internet bewerten.
DigComp 2.2 AT	1.2. Daten, Informationen und digitale Inhalte kritisch bewerten und interpretieren 4.3. Gesundheit und Wohlbefinden schützen

Titel der Übung	**2. DAS GEHÖRT (NICHT) ONLINE**
Ziele der Übung	Einschätzen können, welche Informationen online geteilt werden dürfen. Gefühl für schützenswerte Daten bekommen.
Setting	Einzelcoaching, Gruppenübung
Vorbereitung	Karten für die Diskussion ausdrucken.
Umsetzung	Zu den bereitgestellten Karten wird jeweils diskutiert: In welchem Kontext wäre es okay, diese Information zu veröffentlichen?
Zu beachten	Nur wenige Daten sind eindeutig in der Beurteilung. Bei vielen hängt es davon ab, ob sie öffentlich zugänglich gemacht werden sollen oder im privaten Kreis bleiben.
Unterlagen	Karten mit Fragen im Anhang des Leitfadens
DigComp 2.2 AT	4.2. Personenbezogene Daten und Privatsphäre schützen

Titel der Übung	**3. HEIRATSSCHWINDEL ONLINE**
Ziele der Übung	Ein Bewusstsein dafür entwickeln, dass nicht alle Personen im Internet die Wahrheit sagen. Ein Gefühl für Internetbetrug entwickeln.
Setting	Gruppenübung
Vorbereitung	Fake-Profile aus Facebook, die eventuell für Heiratsschwindel genutzt werden könnten, suchen.
Umsetzung	Falls dies zur Gruppe passt und möglich ist, können Sie eine paradoxe Intervention wählen: miteinander ein Online-Setting für eine Heiratsschwindlerin/einen Heiratsschwindler entwickeln und durchspielen (als Fallstudien). Sollte dies nicht möglich sein, können Sie die Praktiken des Heiratsschwindels durchgehen und diese erklären. In einer zweiten Phase wird in der Gruppe diskutiert, wie Heiratsschwindel entlarvt werden kann. Weiters sollte besprochen werden, wie sich Personen vor solchen Verführungen schützen können.
Zu beachten	Achtung: Sind Personen aus der Gruppe vielleicht schon einmal solchen Heiratsschwindel zum Opfer gefallen, so dürfen diese nicht vorgeführt oder als „naiv“ bezeichnet werden. Sie sind einem professionellen Betrug zum Opfer gefallen und es wurde mit ihren Gefühlen gespielt. Diese Personen brauchen also Unterstützung.
Unterlagen	https://datingfalle.at/
DigComp 2.2 AT	4.4. Sich vor Betrug und Konsumentenrechtsmissbrauch schützen

Titel der Übung	**4. MEINE SPUREN IM NETZ**
Ziele der Übung	Einen Überblick erhalten, welche Informationen über die eigene Person online sind. Wissen, wie man sich einen Überblick über die eigene Online-Darstellung verschaffen kann.
Setting	Einzelcoaching
Vorbereitung	Sofern möglich, die Suchstrategien im Vorfeld ansehen und vorbereiten.
Umsetzung	Die TN suchen nach sich selbst: In der Suchmaschine unter Anführungszeichen, in den sozialen Netzwerken nach Namen und Spitznamen, auf Spieleseiten (an denen sie teilgenommen haben), mit der umgekehrten Bildersuche nach Bildern der eigenen Person etc. Je nach Interessen können weitere Plattformen dazukommen.
Zu beachten	Sollten nachteilige Informationen auftauchen, so ist es wichtig, die TN dabei zu unterstützen, diese auch wieder aus dem Netz zu löschen.
Unterlagen	Broschüre: Persönlichkeitsrechte im Internet
DigComp 2.2 AT	4.2. Personenbezogene Daten und Privatsphäre schützen

Titel der Übung	**5. WAS ICH IM INTERNET NICHT SEHEN WILL**
Ziele der Übung	Mit ungeeigneten Inhalten umgehen können. Wissen, wie man eigene Geräte schützen kann.
Setting	Einzelcoaching
Vorbereitung	Keine Vorbereitung, da dies eher anlassbezogen angesprochen wird.
Umsetzung	Falls von den TN angesprochen, dass sie mit Inhalten online konfrontiert werden, die sie nicht sehen wollen. Dazu zählen Werbung, Gewaltinhalte, pornografische Inhalte etc. In einer ersten Phase wird an den Geräten der TN eruiert, wie es zu diesen Inhalten kommen kann: durch das eigene Verhalten (in der Chronik ersichtlich), durch Kontakte etc. Nun wird überlegt, welche Einstellungen getroffen werden können, damit diese Inhalte weniger wahrscheinlich werden.
Zu beachten	
Unterlagen	https://www.saferinternet.at/services/broschuerenservice/ – Sicherheitseinstellungen für Geräte
DigComp 2.2 AT	4.1. Geräte schützen

ANHANG: KARTEN FÜR ÜBUNG 2. DAS GEHÖRT (NICHT) ONLINE

Name meiner guten Bekannten, mit der ich gerne Prosecco trinke	*Spitzname in meiner Jugend*
Ein Foto meines neugeborenen Enkels	*Ein Foto meiner gehäkelten Einkaufstasche*
Die Anleitung, ein altes Rennrad zu reparieren	*Meine Kontonummer*

ANHANG: KARTEN FÜR ÜBUNG 2. DAS GEHÖRT (NICHT) ONLINE

Meine Sozial-versicherungs-nummer	*Meine Schuhgröße*
Die Größe meines Gartens	*Die Augen-farbe meines Enkelkindes*
Der Beruf meiner Tochter/ meines Sohnes	*Ein Foto von der Eingangstüre meiner Nachbarin/ meines Nachbars*

ANHANG: KARTEN FÜR ÜBUNG 2. DAS GEHÖRT (NICHT) ONLINE

Meine Lieblingsmusik	*Meine Adresse*
Gesundheitliche Probleme meiner Enkelin/ meines Enkels	*Ein Rezept, das ich erfunden habe*
Meine E-Mail-Adresse	*Ein Rezept, das ich vor 20 Jahren aus der Zeitung ausgeschnitten habe*

ANHANG: KARTEN FÜR ÜBUNG 2. DAS GEHÖRT (NICHT) ONLINE