Sicherheit im Internet und am Handy

Welche Gefahren lauern im Netz. Wie kann ich mich dagegen schützen …

Seniorenbund Neumarkt im Mühlkreis

Karl Ortner + Herbert Kohlberger

04. November 2025

Ortsgruppe Neumarkt i. Mkr.

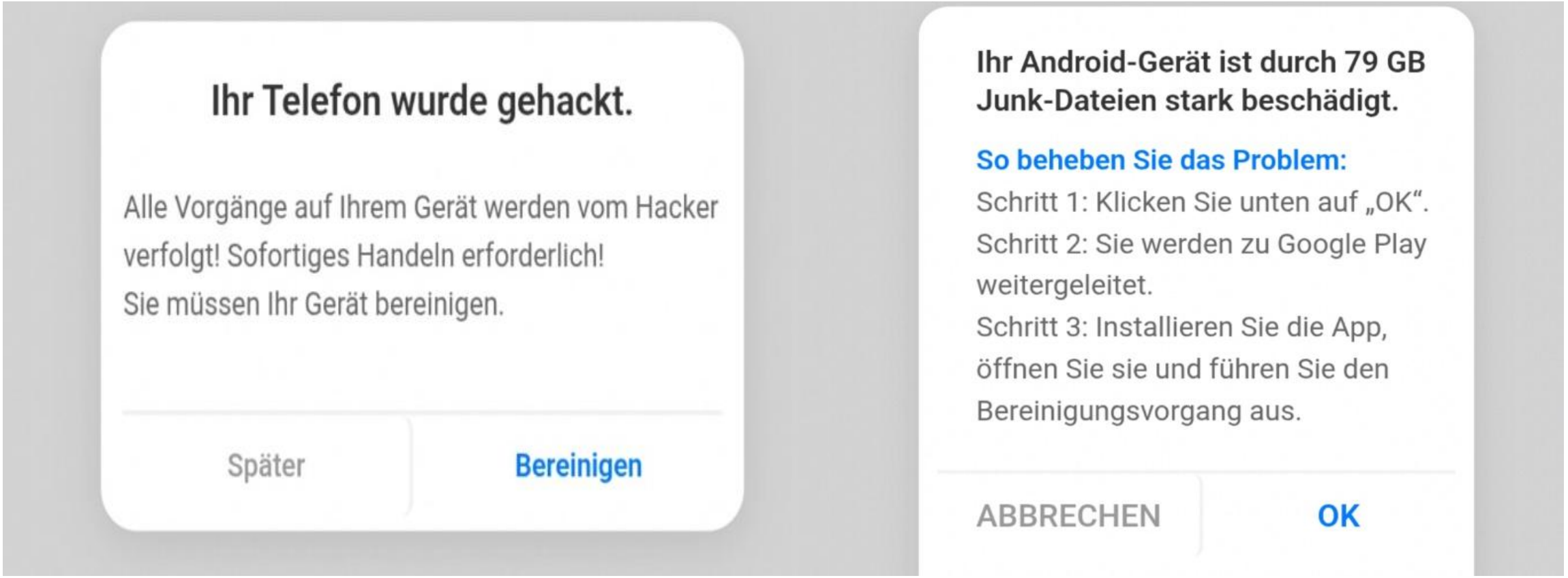
Was wollen wir euch vermitteln:

- Grundlegendes Verständnis für sichere Nutzung von Internet und Handy
- Erkennen von typischen Betrugsversuchen (Phishing, Betrugsanrufe, falsche Apps …)
- Praktische Schutzmaßnahmen kennen und anwenden
- Erkennen, wo Hilfe zu finden ist

Cyber-Kriminalität – Betrug im Internet

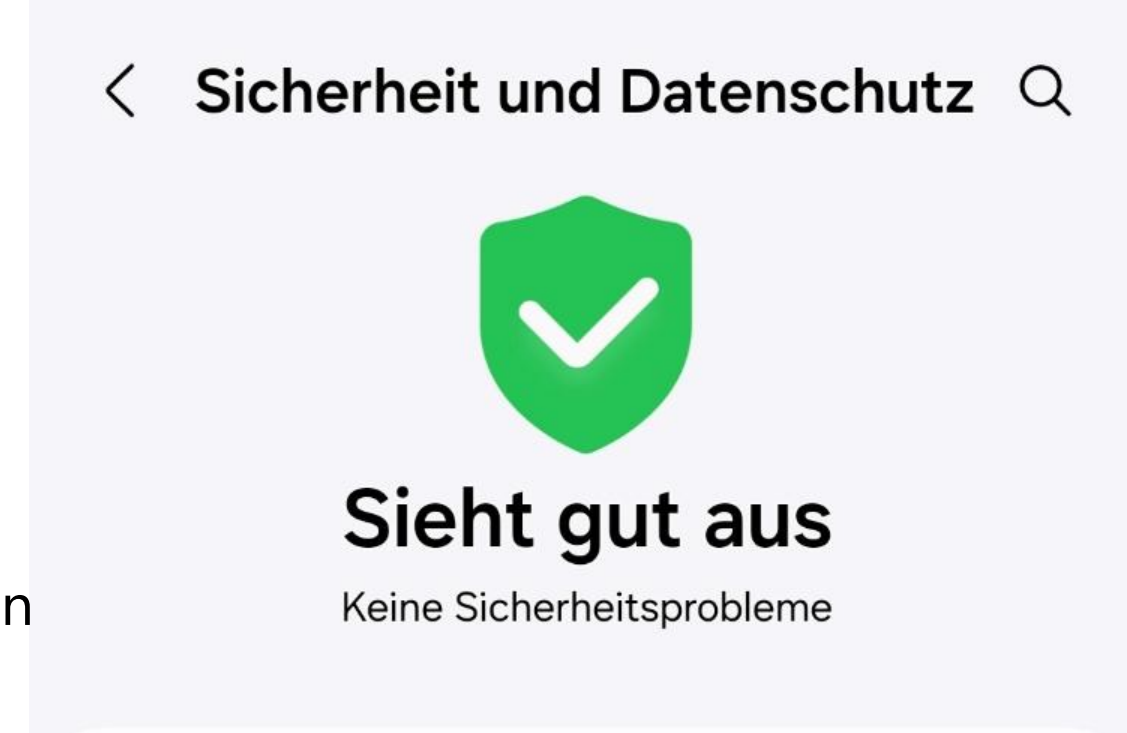
- Über 65.000 Anzeigen in Österreich 2023
- Um das X-fache höher ist die Dunkelziffer, weil sich viele geschädigte schämen zur Polizei zu gehen
- Der Mensch ist die größte Schwachstelle
- 95% sagen: Es trifft eh nur die Älteren und Dummen!
- Die Statistik zeigt: Die meisten Opfer sind älter als 50 und in Führungspositionen
- Viele Nutzer sind sich dieser Bedrohungen möglicherweise nicht bewusst. Es ist wichtig, aufmerksam zu sein und sich über Gefahren im Klaren zu sein

Es poppt am Handy ein Fenster auf …



Was tun?

- 1. Alle Apps schließen!
- 2. Evtl. bei Handy Neustart machen
- 3. Unter Einstellungen schauen > Sicherheit und Datenschutz
- 4. Browser-Cache leeren:
  > Einstellungen | Apps | zB Chrome | unter Speicherplatz | Cache > leeren



Malware (= Schadsoftware)

- *Sammelbegriff für bösartige Programme, die direkt auf dem Gerät installiert werden. Oft landet sie durch Phishing-SMS/Emails oder den Besuch von unsicheren Webseiten auf dem Computer*
- Viren
  - Infizieren andere Programme und verbreiten sich
- Trojaner
  - Als Trojaner bezeichnet man ein Computerprogramm, das als nützliche oder harmlose Anwendung getarnt ist, im Hintergrund aber schädliche Funktionen erfüllt.
- Spyware
  - Überwacht Aktivitäten und stiehlt Daten.

Malware (2)

- Adware
  - Zeigt unerwünschte Werbung an
- Ransomware
  - Ransom ist Englisch und bedeutet Lösegeld. Bei dieser Art von Schadsoftware wird Lösegeld durch die Verschlüsselung von persönlichen Daten erpresst.
- Botnetze
  - Bezeichnen – meist mehrere Tausend – durch Computerviren zusammengeschlossene Computer, die im Verborgenen zu bestimmten Aktionen missbraucht werden. Die Rechenleistung kann zum Beispiel dazu missbraucht werden, wahllos Passwörter zu schon bekannten Email Adressen zu testen

Bedrohungen nach Häufigkeit

- Diese Tabelle zeigt die häufigsten Bedrohungen im Internet.

BEDROHUNG	BEISPIEL	HÄUFIGKEIT
Phishing	E-Mail-Betrug	30%
Malware	Viren und Trojaner	25%
Identitätsdiebstahl	Gestohlene Daten	20%
Ransomware	Krypto-Locker (Computer-Daten werden durch Verschlüsselung unzugänglich gemacht)	15%
Spam	Unerwünschte Werbung	10%

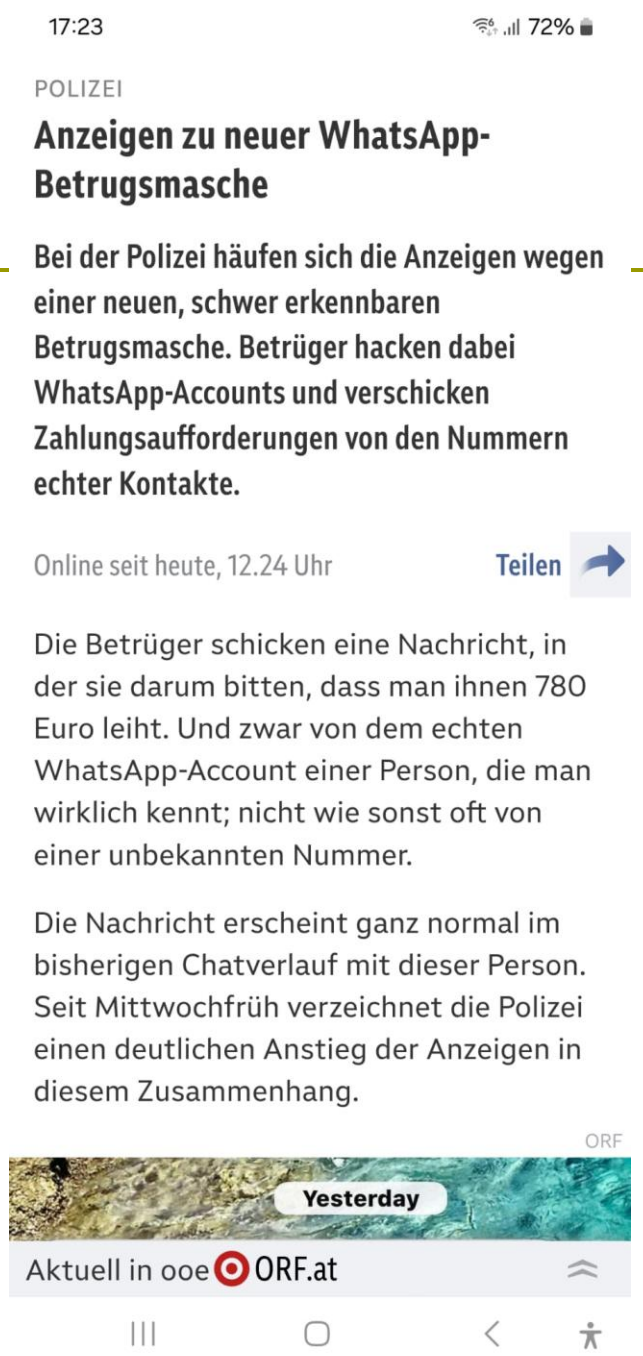
PHISHING

- Mit glaubwürdigen Argumenten wird versucht an sensible Daten zu kommen:

  - Wortkombination aus „Password“ + „fishing“ (angeln)
  - Betrugsversuche, bei denen Angreifer sich als vertrauenswürdige Institutionen ausgeben, um sensible Informationen wie Passwörter, Kreditkartendaten oder persönliche Daten zu stehlen oder sie erschleichen, die Installation von Schadsoftware durch gefälschte Webseiten oder SMS/Emails mit vermeintlich vertrauenswürdigen Absendern.
  - **Beispiele:** Gefälschte E-Mails von Banken oder das Kopieren von vertrauenswürdigen Webseiten *(Sie loggen sich z.B. mit Ihren Bankdaten ein und die Betrüger lesen mit)*, Fake-SMS der Paketdienste *(Es wird ein Link zugesendet, um einen bestimmten Betrag zu überweisen, wobei dann Ihre Kreditkartendaten gestohlen werden).*

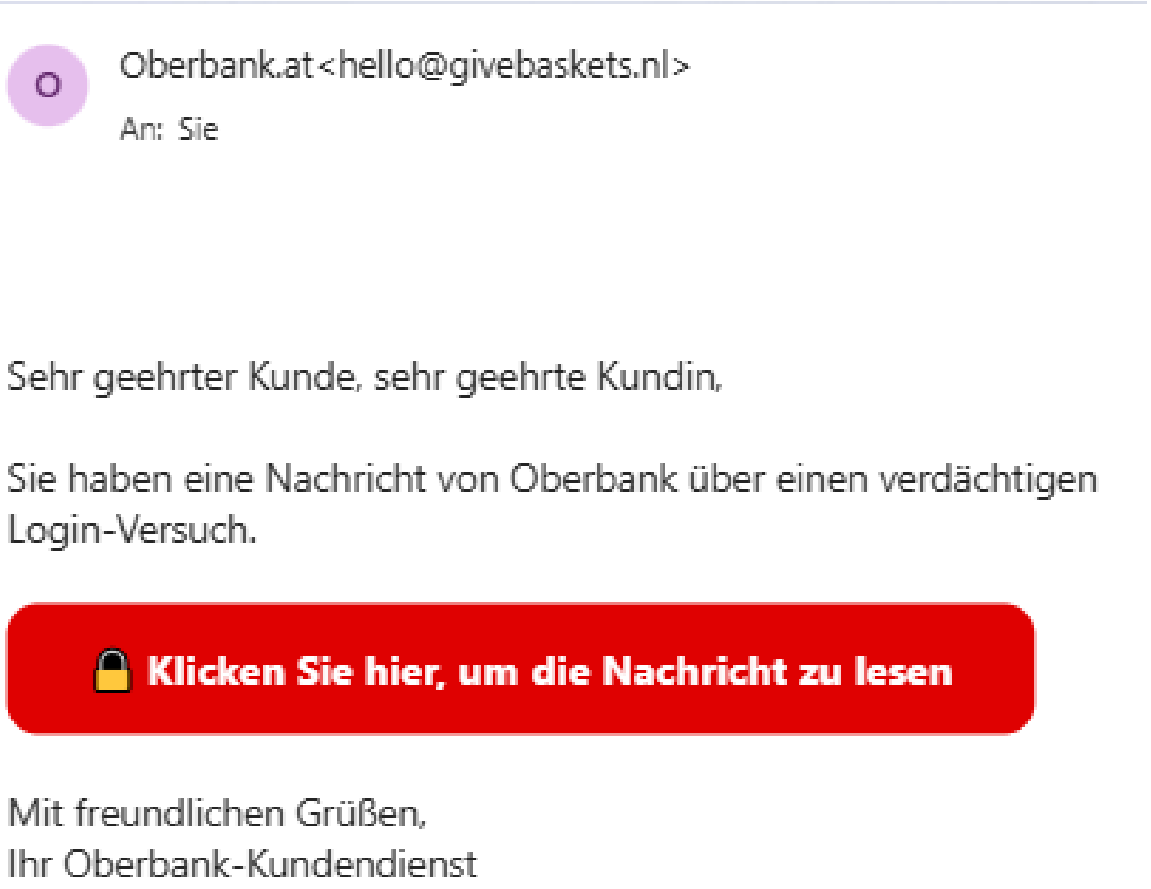
Phishing-Beispiele

- Aktuelle Bedrohung > Whats-App-Account gehackt -Versand von Zahlungsauf-forderungen von Nummern echter Kontakte !!



Phishing-Beispiele

- Emails von Banken: verdächtige Login-Versuche !!
- Absender > hello@givebaskets.nl



Phishing-Beispiele

- Email-Empfänger unter BCC
- > Massenemails auf Verdacht

M

Mietrückstand
22. Oktober 2025 13:39
Details ausblenden

Von "Mietrückstand" <verwaltungimmobilien.at@gmail.com>

An info@immobilienverwaltung.gv.at

BCC karlortner@gmx.at

Nachrichtendetails

Sehr geehrte Mieter,

Nach Überprüfung stellen wir fest, dass die Zahlung Ihrer Miete für Oktober August noch nicht erfolgt ist, obwohl die Frist bereits abgelaufen ist. Um Verzugsgebühren und mögliche Inkassomaßnahmen zu vermeiden, bitten wir Sie, die Zahlung so schnell wie möglich vorzunehmen.

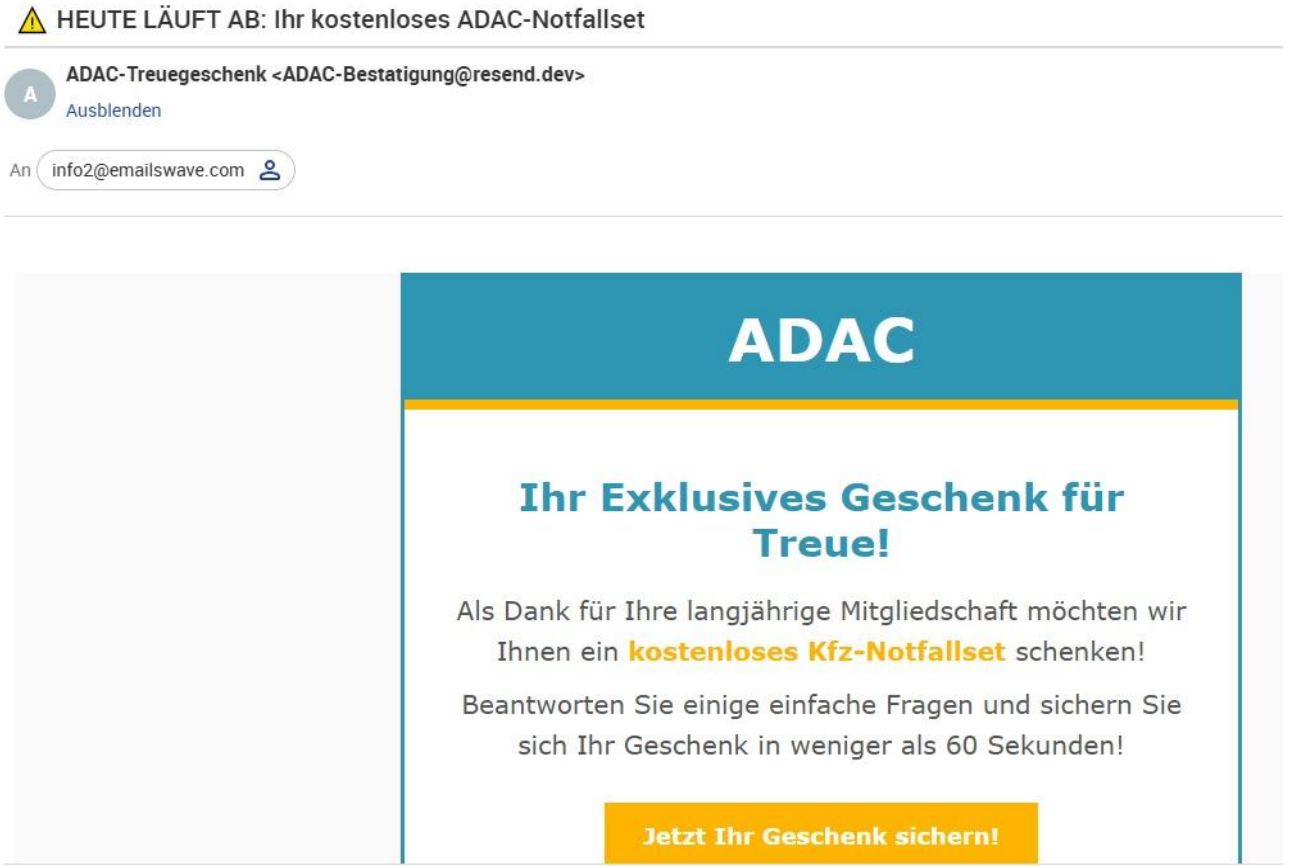
Darüber hinaus möchten wir Sie darüber informieren, dass sich unsere Bankverbindung geändert hat. Wir wären Ihnen dankbar, wenn Sie uns den Erhalt dieser Nachricht bestätigen würden, damit wir Ihnen unsere neuen Bankdaten (RIB) übermitteln können.

Wir bitten Sie, diese Situation so schnell wie möglich zu bereinigen und stehen Ihnen für dringende Fragen gerne zur Verfügung.

Bitte senden Sie uns eine E-Mail, damit wir Ihnen unsere neuen Bankdaten zusenden oder Ihnen die neuen Zahlungsmodalit mitteilen können.

Phishing-Beispiele

- Mails von ÖAMTC / ADAC: locken mit Geschenken bei Antwort auf die Mail



Phishing – Fake Shops

- Fake-Shops-Angebote nehmen zu (oftmals KI-generiert)
  - Black-Friday > elektr. Geräte
  - Tickets für Events
  - Lebensmittelgeschäfte (Hofer, Billa etc.)

Polizei warnt vor Internetbetrug mit Holzpellets

Betrüger behalten Vorauszahlungen ein, ohne Ware zu liefern – und locken mit extrem günstigen Preisen

SANKT PÖLTEN. In der kalten Jahreszeit haben Bestellbetrügereien Hochsaison. Die Polizei warnt vor Fake-Onlineshops beim Kauf von Pellets und anderen Heizmaterialien wie Briketts und Brennholz. Derzeit werde vermehrt mit einer Betrugsmasche agiert, bei der Vorauszahlungen von Kunden einbehalten werden, ohne dass Ware geliefert wird.

„Cyber-Kriminelle locken mit extrem günstigen Preisen und einer professionell wirkenden Website", teilte die Landespolizeidirektion Niederösterreich am Montag anlässlich der beginnenden Heizsaison in einer Aussendung mit.

Fake-Shops bieten Holzpellets zu ungewöhnlich günstigen Preisen an. Symbolbild: cb

„Starkes Alarmzeichen"

Geraten wurde, misstrauisch zu bleiben und den Anbieter zu überprüfen. Fehlt ein Impressum oder sind die Angaben unvollständig oder unglaubwürdig, sollte dort nicht eingekauft werden. Um Warnungen und Erfahrungsberichte zu finden, sollte in einer Suchmaschine der Name des Anbieters zusammen mit Begriffen wie „Betrug", „Fake", „Erfahrung" oder „Problem" eingegeben werden. „Extreme Preisnachlässe und Angebote, die weit unter dem marktüblichen Durchschnitt liegen, sind ein starkes Alarmzeichen für einen Fake-Shop", hieß es weiters.

Werden am Beginn des Bestellvorgangs verschiedene Zahlungsmethoden angeboten und ist am Ende ausschließlich Vorkasse per Banküberweisung möglich, sollte der Kauf sofort abgebrochen werden. Eine Überweisung im Voraus biete Kunden keinerlei Schutz.

Direkt über Plattform abwickeln

Bei Käufen über Kleinanzeigenplattformen versuchen Betrüger laut Exekutive oft, die Sicherheitsvorkehrungen des Portals zu umgehen, und weichen auf E-Mail oder WhatsApp aus. Die Bestellung sollte immer direkt über die Plattform abgewickelt werden, rät die Polizei: „Weigert sich die Verkäuferin oder der Verkäufer, ist das ein klares Alarmsignal."

Die kalte und finstere Jahreszeit ruft nicht nur Bestellbetrüger verstärkt auf den Plan, sondern auch moderne Heiratsschwindler, warnen Kriminalisten. Dabei nehmen die Täter im Internet Kontakt zu ihren späteren Opfern auf und gaukeln ihnen die große Liebe vor.

- Shop prüfen: Suchmaschine „Fake-Shop Detector". Ist das Impressum plausibel, sind Preise realistisch?
- zB

Phishing – erkennen / löschen

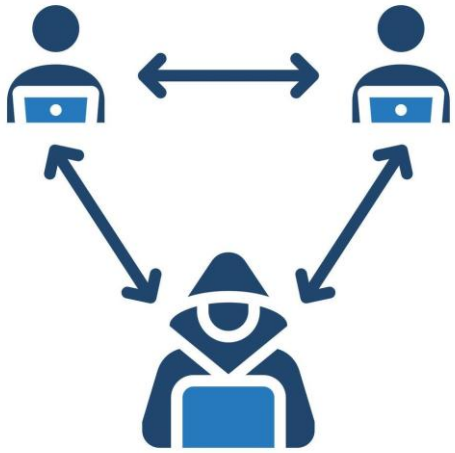
- Prüfungen bei Phishing-Mails
  - Eine Mail zu öffnen, ist noch kein Problem
  - Absender überprüfen: auf Absender klicken > Details einblenden
  - Keinen Anhang öffnen
  - Rechts oben auf … „Drei-Punkte-Auswahlfeld“ gehen
    > Spam melden & blocken.
  - Spam-Ordner laufend leeren

Social-Engineering (soziale Manipulation)

- Beeinflussungen – oft ohne den Einsatz von Technologie - mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen. Die Täter geben vor, eine vertraute Person zu sein. Beispielweise über gehackte Facebook-Konten von Freunden. Die Opfer werden dazu gebracht, selbstständig wichtige Daten preiszugeben oder Schadsoftware zu installieren.

- **Beispiele:** Telefonanrufe, bei denen Betrüger sich als Support-Mitarbeiter ausgeben.

Man-in-the-Middle-Angriffe (MitM)



- Abfangen und Manipulieren der Kommunikation zwischen zwei Parteien, oft ohne dass die Opfer es merken.
- **Beispiele:** Abhören von Daten in öffentlichen WLAN-Netzwerken.
- **Wie schütze ich mich?** Nie in öffentlichen Netzwerken z.B. in Internetcafes oder auf Banken einloggen bzw. Geldtransfers vornehmen!

SPAM-Mails

- „unerwünschte“ oder „unverlangt“ zugesandte E-Mails. Diese können als „Massenware“ oder als personalisierte Werbemails auftreten.
- Unverlangte E-Mails können Schadprogramme enthalten oder Betrugsversuche einleiten
  - „Ihr Paket konnte nicht zugestellt werden“
  - „Sie haben gewonnen“
  - „Ihr Konto wurde gesperrt“
  - „Ganz einfach € 5.000.- im Monat verdienen
- Laut Angaben ist der Spam-Anteil **größer als 95 %** in der E-Mail-Infrastruktur !!
- Prüfung der Spam-Mails wie bei „Phishing-Mails“ (Spam-Filter setzen)

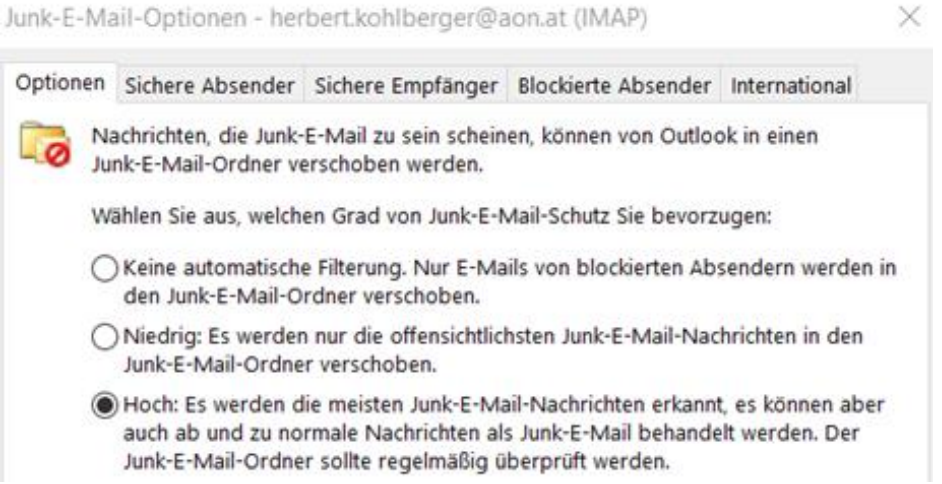
SPAM over Mobile Phone (SPOM)

- Auch die Kommunikation per Mobiltelefon wird von Spam beeinträchtigt. Unerwünschte Kurzmitteilungen oder Anrufe werden als *(Mobile) Phone Spam*, teils auch als *Spam over Mobile Phone (SPOM)* bezeichnet. Verstärkter Einsatz von Mobile Marketing zur Marktforschung oder durch unerwünschte Kurzmitteilungen. Eine Variante sind sogenannte *Spam-* oder *Ping-Anrufe*, die nur Sekundenbruchteile dauern und den Angerufenen zum teuren Rückruf eines Mehrwertdienstes verleiten sollen.

  Mehrwertnummern in Österreich sind spezielle Telefonnummern, die zusätzliche Gebühren für Dienstleistungen erheben, und sie sind mit den Vorwahlen 0810, 0820, 0821, 0900, 0901, 0930, 0931, 0939 und 118 verbunden.

- Definition: *https://de.wikipedia.org/wiki/Spam*

Wie kann ich mich schützen



- Im Mailprogramm Spamfilter aktivieren (je nach Mailprogramm. Bei Outlook ALT unter „Start/Junk-Email/Junk-Mail-Optionen)
- Inhalt hinterfragen (speziell bei Emails kritisch sein)
- Keine Anhänge öffnen (nicht automatisch einfach öffnen)
- Keine Programme herunterladen bei fragwürdigen Webseiten
- Auf **https://** oder versperrtes Schloss-Symbol achten
- Sichere Passwörter (mind. 8 Zeichen mit Zahlen und Sonderzeichen)
- Jede unaufgeforderte Mail als Junk/Spam markieren/melden (rechte Maustaste auf E-Mail)

Handy-Sperre mit Face-ID

- Gesichtserkennung am Samsung bzw. Android.
- Ähnlich wie Apple nutzt auch Android die biometrischen Gesichtsdaten, um den Zugriff auf das Gerät zu gewährleisten. So einfach geht’s:

1. Öffnen Sie die Einstellungen Ihres Smartphones.
2. Gehen Sie anschließend auf „Biometrie und Sicherheit“.
3. Tippen Sie auf „Gesichtserkennung“ und folgen Sie der Anleitung auf dem Display.

- Wer den Fingerprint bevorzugt, wählt den gleichen Vorgang.

Fake News – was ist das?

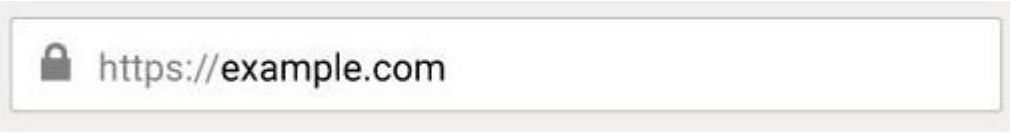
- Der Begriff „Fake News“ bezeichnet Falschmeldungen, die gezielt vor allem im Internet und hier besonders in sozialen Netzwerken verbreitet werden.
- Die Absichten, die hinter dieser Verbreitung stecken, unterscheiden sich ebenso wie die Art und der Inhalt der Nachrichten. Während manche Fake News harmloser Natur sind, dienen andere dazu, die kritische Meinungsbildung zu beeinflussen und Stimmung geben eine bestimmt Sache zu machen (z.B. Amerikanischer Präsidentschaftswahlkampf).
- Fake News kommen als Push-Nachrichten aufs Handy.
- Fake News poppen beim Stöbern im Internet als Anzeigen oder Inserts in Texten auf.
- **Aktuelles Beispiel** bei Meinungsbeeinflussung ist Elon Musk mit seinem Netzwerk „X“

Fake News – wie erkennen?

- Obwohl viele Fake News auf den ersten Blick täuschend echt wirken, lassen sich die meisten Falschmeldungen durch ein paar einfache Methoden entlarven. Je häufiger Sie die unten genannten Strategien anwenden, desto einfacher fällt es Ihnen, Fake News von echten Nachrichten zu unterscheiden.
  - Gestaltungsmerkmale: Wie ist die Nachricht gestaltet?
  - Hat er einen blauen Verifizierungshaken? (Instagram)
  - Herkunft prüfen: Wer ist der/die/Autor/-in? Gibt es ein Impressum? Wie viele Follower und Freunde hat der Account?
  - Quellenrecherche: Was sagen andere Quellen?
  - Suchmaschinencheck: Wo liegt der Ursprung einer Meldung?
  - Zahlen und Fakten: Sind die Informationen plausibel und aktuell?
  - TIPP: Überprüfung bei Faktencheckern wie bei Mimikama oder Hoaxmap
  - Bilder, Videos und Audio-Dateien: Fälschungen technisch prüfen (zB Google Bilder Suche)

Gefälschte Websites - Erkennung

- Auf die URL schauen: Oft ändern Betrüger die URL nur minimal ab, z.B. „amaz0n.com“ oder eine andere Domain, z.B. „amazon.org“ statt „amazon.com“
- Auf das Schloss achten! Trägt eine Website das Vorhangschloss-Symbol? Dann ist die durch ein TSL/SSL-Zertifikat geschützt.



- **Website von einem Tool prüfen lassen:** Sollten Sie Zweifel an der Sicherheit einer Website beschleichen, nutzen Sie einen Website-Checker (z.B. *https://transparencyreport.google.com/safe-browsing/search*)
- Die Sicherheitsprüfung zeigt etwaige Schwachstellen der Website auf, ebenso ob sie Verschlüsselung nutzt und wie umfangreich die Verifizierung ist.

Gefälschte Websites – was tun?

- **Was sollten Sie tun, wenn Sie einer gefälschten Website begegnen?**

  - Wenn Sie auf einer gefälschten Website gelandet sind, geben Sie keinesfalls sensible Informationen heraus wie Kontodaten, Anmeldedaten (z. B. für Facebook), Bestätigungscodes oder gar Ihren Namen und Ihre Kontaktdaten. Geben Sie einfach nichts an, wenn Ihnen Zweifel kommen. Klicken Sie außerdem nicht auf Links in E-Mails, Online-Beiträgen oder Direktnachrichten von Unbekannt.

  - Melden Sie bestenfalls gefälschte Websites bei Google Safe Browsing und schließen Sie sofort das Browserfenster.

Gefälschte Websites – weitere Tipps

- Wenn Sie nach einem Schloss und Website-Siegel geschaut und die URL in einen Website-Checker eingegeben haben, können Sie die Website auch auf die folgenden vertrauensbildenden Eigenschaften abklopfen:

  - Gibt es eine Datenschutzerklärung
  - Rückgabebedingungen
  - Kontaktdaten des Unternehmens, z. B. Telefonnummer und Anschrift
  - Korrekte Schreibung und Grammatik
  - Online-Bewertungen (suchen Sie im Internet einfach nach „Bewertungen von [Name der Website]“, um sich danach umzuschauen)
  - Halten Sie sich stets von Angeboten fern, die zu gut klingen, um wahr zu sein, denn das sind sie meist auch.

Internetabzocke

- Einladende Internetseiten locken mit vermeintlichen „Gratis“-Angeboten, wie z.B. Gratis-SMS, Spielen, Routenplanern, Outlet-Waren, Rezepten, Software-Downloads etc.
  - Information, dass dafür sehr wohl Kosten anfallen, wird – wenn überhaupt ersichtlich – im Kleingedruckten der AGB versteckt. Es reicht eine Registrierung mit ein paar persönlichen Daten und schon kommen in einigen Wochen Zahlungsaufforderung bzw. Mahnungen.
  - In sozialen Medien wie Facebook, Instagram etc.: An Pyramiden- oder Schneeballsystem teilnehmen
  - Anlagetipps: Es tauchen Fake-Kryptobörsen auf, die sehr raffiniert nachgemacht werden
  - Gefälschte Websites: Es häufen sich perfekt nachgemachte Websites von bekannten Firmen und Institutionen, die nur eines wollen: an ihre Bankdaten kommen.

IoT-Bedrohungen (Internet of Things)

- **Was sind IoT-Geräte?**

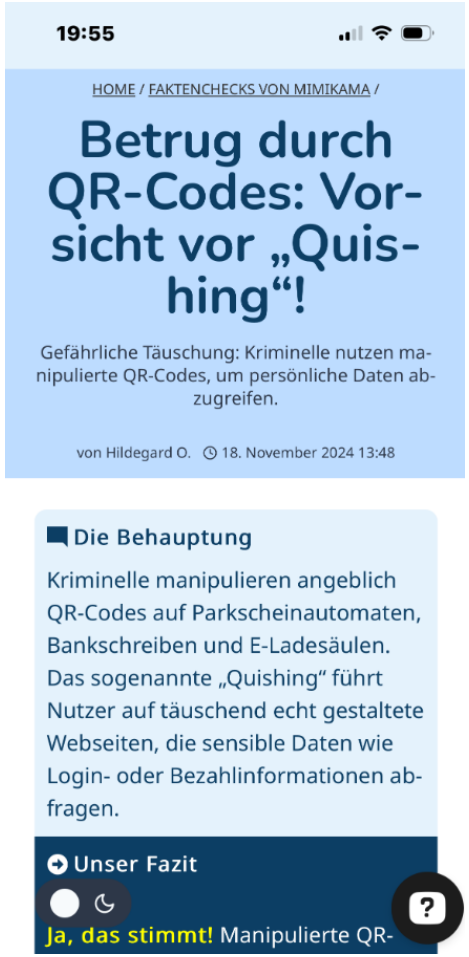
- (Internet der Dinge) sind physische Objekte, die mit Sensoren, Software und Netzwerkkonnektivität ausgestattet sind. Sie können Daten sammeln, speichern und an andere Geräte oder Systeme übertragen. Diese Geräte ermöglichen es, Prozesse zu automatisieren und menschliches Eingreifen zu minimieren

IoT-Bedrohungen (Internet of Things)

- Angriffe auf schlecht gesicherte IoT-Geräte wie Kameras, Smart-Home-Geräte, intelligente Thermostate, Router, medizinische Geräte etc. Bestenfalls Hilfe durch *Profis*!
- In einem durchschnittlichen Smart Home sind zahlreiche Geräte permanent online und miteinander vernetzt. Diese Konnektivität - während sie Bequemlichkeit und Effizienz bietet - öffnet auch Tür und Tor für potenzielle Sicherheitsrisiken. Cyberangriffe können nicht nur die Privatsphäre gefährden, sondern auch physischen Schaden anrichten, wenn etwa durch eine manipulierte Heizungssteuerung Extremtemperaturen verursacht werden.
- Grundlegende Sicherheitsmaßnahmen:
  - Stets aktuelle Software
  - Sichere Passwörter
  - Zwei-Faktor-Authentifizierung (neben PW eine zweite Bestätigung – wie Code auf Smartphone)
- Feststellung, ob ein IoT-Gerät kompromittiert wurde:
  - ungewöhnliche Aktivitäten, wie Neustarts, unerwartete Benachrichtigungen oder ungewöhnlicher Datenverkehr

Quishing – Betrug durch QR-Codes

- Neueste Bedrohung
- Manipulierete QR-Codes, um persönliche Daten abzugreifen, zB auf Parkscheinautomaten etc.
- Grundsätzliche Info, dass es nichts gibt, was es nicht gibt !!



Links zu

- https://www.phishen-impossible.at/
- https://www.saferinternet.at/
- https://www.watchlist-internet.at/ (über whatts-app / Aktuelles)
- https://www.oesterreich.gv.at/themen/onlinesicherheit_internet_und_neue_medien/

- https://www.onlinesicherheit.gv.at/
- https://www.ombudsstelle.at/

Offene Themen / Fragen?

- …
- …?

Digitaler Nachlass: Kommunikation mit Angehörigen und Erben

Wichtigkeit offener Gespräche

Offene Kommunikation klärt Erwartungen und bereitet Erben auf den digitalen Nachlass vor.

Vermeidung von Konflikten

Transparente Gespräche helfen, Missverständnisse und Konflikte unter Erben zu vermeiden.

Erleichterung der Nachlassverwaltung

Klare Kommunikation erleichtert die Verwaltung und Übergabe des digitalen Nachlasses.

Digitaler Nachlass

- Beim digitalen Nachlass handelt es sich insbesondere um die Benutzerkonten und persönlichen Daten, die nach dem Tod eines Menschen im Internet weiter bestehen. *Dazu zählen z.B: >> nächste Folie*

- Auch Offline-Daten, die auf einem Gerät gespeichert sind (wie z.B. Fotos, Videos, Filme, Musik-Dateien, elektronische Dokumente etc.), gehören zum digitalen Nachlass.

- Die Erben treten nach der Einantwortung in alle Rechte, Pflichten und Rechtsverhältnisse der/des Verstorbenen ein. Auch im Internet geschlossene Verträge der/des Verstorbenen gehen also auf die Erben über.

Abgrenzung zu klassischem Nachlass

Klassischer Nachlass

Der klassische Nachlass besteht aus physischen Gegenständen wie Immobilien, Schmuck oder Bargeld.

Digitaler Nachlass

Digitaler Nachlass umfasst elektronische Daten wie E-Mails, Cloud-Speicher und Online-Konten.

Verwaltung und Vererbung

Die Verwaltung digitaler Daten benötigt spezielle Regelungen und technisches Fachwissen.

Digitaler Nachlass:>> Dazu zählen zB

- Profile auf sozialen Netzwerken (Facebook, X, Xing, LinkedIn etc.)
- E-Mail-Konten
- Konten bei Online-Diensten (PayPal, Spotify, Netflix etc.)
- Blogs, Websites, Domainnamen
- Online-Banking
- Mediendienste (Spotify, Netflix, Online-Abos von Zeitungen etc.)
- Fotodienste (Instagram, Flickr)
- Videodienste (YouTube, Vine etc.)
- Versandhandel (Amazon, eBay etc.)
- Profile auf Partnervermittlungsbörsen
- E-Government (FinanzOnline, ID Austria, etc.)

Datenschutz und Persönlichkeitsrechte

Datenschutz nach dem Tod

Datenschutzbestimmungen bleiben nach dem Tod wirksam und schützen die digitalen Daten des Verstorbenen.

Bedeutung für Erben

Erben müssen Datenschutz- und Persönlichkeitsrechte beachten, um rechtliche Konflikte zu vermeiden.

Schutz der Privatsphäre

Der Schutz der Privatsphäre des Verstorbenen bleibt zentral im Umgang mit digitalen Daten nach dem Tod.

Digitaler Nachlass: Vorsorge

Grundsätzlich gibt es folgende vier Möglichkeiten, mit dem digitalen Nachlass umzugehen:

- Erhaltung
- Löschung
- Archivierung
- Übertragung der Daten an Angehörige/Erben/dritte Personen

Digitaler Nachlass: Vorsorge

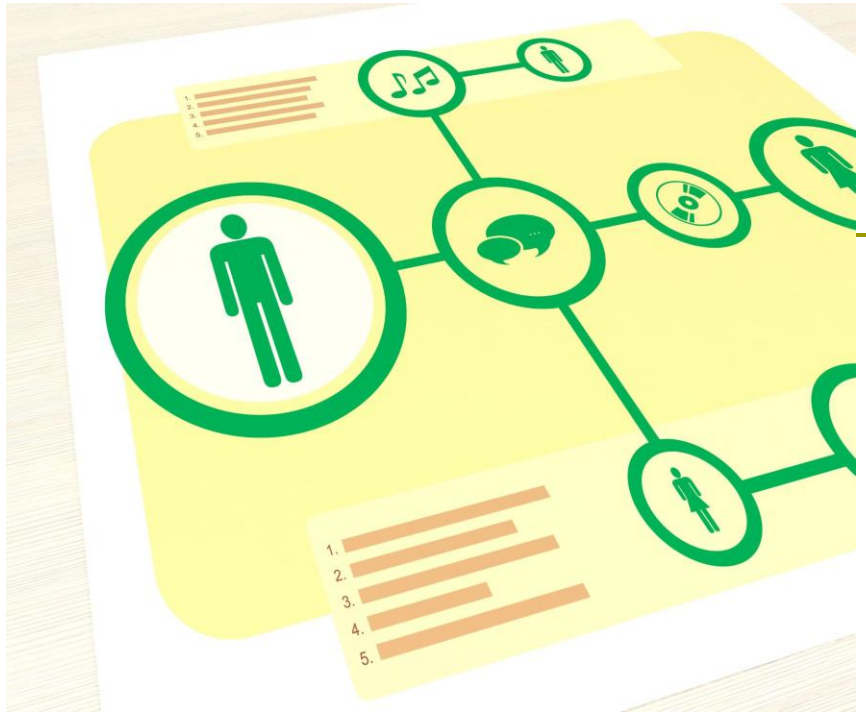
- Die meisten sozialen Netzwerke **(Facebook, Instagram etc.)** bieten mittlerweile Optionen an, um für den Todesfall vorzusorgen. So gibt es beispielsweise die Möglichkeit einzustellen, dass bestimmte Personen informiert werden, wenn die Kontoinhaberin/der Kontoinhaber über längere Zeit inaktiv ist bzw. eine Person als "**Nachlasskontakt**" festzulegen. Informationen dazu finden sich unter den Kontoeinstellungen des jeweiligen sozialen Netzwerks.

- Eine technische Alternative zur physischen Liste der Zugangsdaten ist die Verwendung eines **Passwort-Managers.** Ein Passwort-Manager ist ein Programm, in dem alle Zugangsdaten (Benutzernamen, Passwörter) gespeichert und mit einem einzigen Hauptpasswort abgerufen werden können. Eine Vertrauensperson kann im Todesfall mit dem einzigen Hauptpasswort alle Zugangsdaten abrufen.

Digitaler Nachlass: Vorsorge

- Eine Liste mit allen Online-Mitgliedschaften, Profilen und sonstigen Accounts, gegebenenfalls inklusive **Benutzernamen und Passwörtern**, ist die wichtigste Vorsorge für den digitalen Nachlass. Diese Liste sollte an einem sicheren Ort verwahrt werden (Dokumentenmappe) oder eventuell sogar bei einer Notarin/einem Notar hinterlegt werden.

- Empfehlenswert ist es, neben den Zugangsdaten auch die gewünschte Vorgehensweise für die Hinterbliebenen zu hinterlegen und bestenfalls mit seinen Vertrauten zu besprechen.



Festlegung von Verfügungsanweisungen

Klare Anweisungen festlegen

Der Erblasser bestimmt eindeutig, wie seine digitalen Daten und Konten nach seinem Tod verwaltet werden sollen.

Rechtliche Dokumentation

Verfügungsanweisungen können im Testament oder in separaten Dokumenten geregelt werden, um Rechtsklarheit zu schaffen.

Vermeidung von Streitigkeiten

Klare Verfügungsanweisungen helfen, spätere Konflikte und Streitigkeiten unter Erben zu vermeiden.

Umgang mit dem digitalen Nachlass eines Verstorbenen **OHNE** Vorsorge

Wurde **keine** **Vorsorge** bezüglich des digitalen Nachlasses getroffen und die/der Verstorbene hat **keine Aufzeichnungen ihrer/seiner Online-Aktivitäten hinterlassen**, gibt es einige Tipps für Hinterbliebene, um die Online-Aktivitäten ermitteln und gegebenenfalls Schritte setzen zu können

- Mit Internetsuchmaschinen (Google) kann nach dem Namen oder E-Mail-Adressen der/des Verstorbenen gesucht werden. Auch nach Spitznamen oder Namenskürzeln sollte gesucht werden.

- Freundinnen/Freunde, Verwandte, Kolleginnen/Kollegen sowie die Partnerin/der Partner sollten zu den Online-Aktivitäten der/des Verstorbenen befragt werden.

Umgang mit dem digitalen Nachlass eines Verstorbenen **OHNE** Vorsorge

Wenn der digitale Nachlass identifiziert wurde, können die einzelnen Dienste bzw. Netzwerke kontaktiert und über den Todesfall benachrichtigt werden. In der Regel wird die Sterbeurkunde, oft aber auch die Einantwortungsurkunde, benötigt. Um Missbrauch auszuschließen, prüfen die Unternehmen solche Anträge in der Regel genau, was Zeit in Anspruch nimmt.

- Zugriff auf E-Mail-Konten
  - Bei einigen E-Mail-Anbietern können die Hinterbliebenen einen Antrag auf Zugriff auf den Account der/des Verstorbenen stellen. Für den Antrag werden auch hier meist die Sterbeurkunde und die Einantwortungsurkunde benötigt.
- Social Media
  - Die meisten sozialen Netzwerke (Facebook, Google+ etc.) bieten mittlerweile Optionen an, mit dem Konto einer verstobenen Person umzugehen. Auf Facebook kann beispielsweise ein Antrag auf Herstellung des Gedenkzustands gestellt werden. Informationen dazu finden sich auf den Hilfe-Seiten des jeweiligen sozialen Netzwerks.

Digitaler Nachlass: Checkliste

- Erstellung eines Dokuments mit folgenden Informationen:
  - Welche Daten/Accounts/Online-Mitgliedschaften etc. gibt es?
  - Wie lauten die jeweiligen Zugangsdaten?
  - Was soll mit dem jeweiligen Account/den jeweiligen Daten geschehen (Erhaltung/Löschung/Archivierung/Übertragung der Daten an eine andere Person)?
  - Wer soll sich darum kümmern?

- Verwahrung des Dokuments an einem sicheren Ort, der den Hinterbliebenen bekannt ist.

- Broschüre „Digitaler Nachlass“ Link:
  https://www.ispa.at/wissenspool/broschueren/broschueren-detailseite/broschuere/detailansicht/digitaler-nachlass

Fazit:
Digitalen Nachlass verantwortungsvoll gestalten

Frühzeitige Planung

Eine frühzeitige Planung ist essenziell, um den digitalen Nachlass kontrolliert und sicher zu regeln.

Rechtliche Klarheit

Klare rechtliche Regelungen helfen, Konflikte zu vermeiden und den Nachlass eindeutig zu gestalten.

Moderne Tools nutzen

Der Einsatz moderner Tools unterstützt die sichere Verwaltung und Nachvollziehbar-keit des digitalen Nachlasses.

Erleichterter Übergang

Ein gut gestalteter digitaler Nachlass sichert das Erbe und erleichtert den Übergang für Erben.

oösb
Ortsgruppe
Neumarkt i. Mkr.