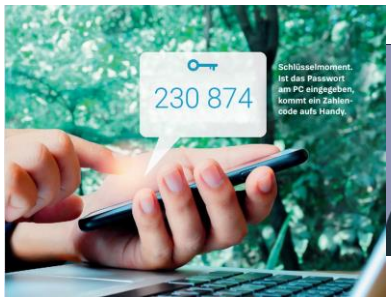
DigiSmart-2025

Passwörter und Notruf (oder Notfallpass)
und Weihnachtselfen zum Jahresende

Das Letzte für 2025!
Das Thema OnlineKonten zieht Kreise. Es ist dringend erforderlich, über Passwörter zu reden. Das wollen wir heute tun.
Und dann ist uns noch wichtig, euch an den Notfallpass in eurem Handy zu erinnern.
Und wir wünschen natürlich frohe Weihnachten – mit einem lange einstudierten Tanz ;-)
Viel Spaß im heutigen Kursmodul.

Warum sichere Passwörter so wichtig sind

- Passwortsicherheit
- 2-Faktor-Authentifizierung



16.12.2025 Christiane Stadtfeld - Anita Velten 2

Warum sichere Passwörter so wichtig sind

Hier ein paar Infos zum Verstehen:
Datenlecks entstehen, wenn **vertrauliche Informationen unbeabsichtigt oder durch Angriffe nach außen gelangen**. Das kann auf verschiedene Arten passieren – oft ist es eine Kombination aus Technik **und** menschlichen Fehlern.
Datenlecks entstehen, wenn **vertrauliche Informationen unbeabsichtigt oder durch Angriffe nach außen gelangen**. Das kann auf verschiedene Arten passieren – oft ist es eine Kombination aus Technik **und** menschlichen Fehlern.
Datenlecks entstehen selten durch einen einzigen Fehler – sondern durch eine Kette kleiner Nachlässigkeiten

Die häufigsten Ursachen von Datenlecks
1. Hackerangriffe - Angreifer nutzen Sicherheitslücken aus, z. B.: ungepatchte Software, schlecht gesicherte Server, schwache oder gestohlene Admin-Passwörter
👉 Ergebnis: **Datenbanken mit E-Mails, Passwörtern oder Zahlungsdaten werden kopiert.**
2. Schwache oder wiederverwendete Passwörter

Passwort zu einfach („123456“, „Passwort“)
Dasselbe Passwort auf mehreren Seiten
➡️ Wird **eine** Seite gehackt, können Angreifer viele andere Konten ausprobieren (Credential Stuffing).

3. Phishing (sehr häufig!)

Täuschende E-Mails oder Webseiten: sehen aus wie von Banken, Paketdiensten oder Social Media
fordern dich auf, dich „dringend“ einzuloggen.
>> Wenn man dort sein Passwort eingibt, gibt man es **direkt den Angreifern**.

4. Menschliche Fehler

Ganz banal, aber extrem häufig: falscher E-Mail-Empfänger, öffentlich zugängliche Cloud-Ordner, sensible Daten in GitHub-Repos hochgeladen

5. Unsichere Speicherung von Daten

Passwörter im Klartext gespeichert ❌, schlechte oder veraltete Verschlüsselung, fehlende Zugriffsbeschränkungen.
Wenn so ein System kompromittiert wird, sind **alle Daten sofort lesbar**.

6. Malware & Keylogger

Schadsoftware kann: Tastatureingaben mitschneiden, Passwörter aus Browsern auslesen, Sitzungen übernehmen

Oft eingeschleust durch: infizierte Downloads

E-Mail-Anhänge, gefälschte Software

7. Drittanbieter & Lieferketten

Ein Dienst nutzt andere Dienste: Zahlungsanbieter, Analyse-Tools, Cloud-Dienste
➡️ Wird ein **Partner** gehackt, können **deine Daten indirekt betroffen** sein.

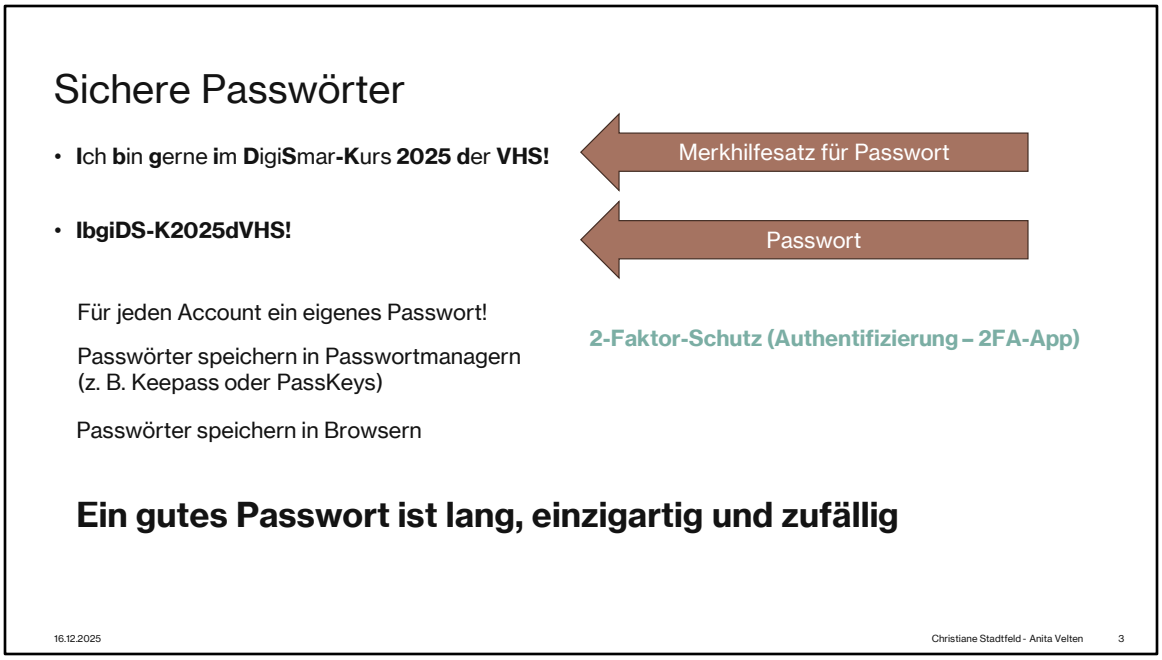
Was passiert mit den Daten?

Verkauf im Darknet, Spam & Betrug, Identitätsdiebstahl, Kontoübernahmen

Wie kann man sich schützen? (Kurzfassung)

✅ **Einzigartige Passwörter**
✅ **Passwort-Manager**
✅ **2-Faktor-Authentifizierung**
❌ Keine Klicks auf verdächtige Links
🔄 Software aktuell halten

s. Authentifizierungs-Apps-test-11-2024.pdf



Wie erstelle ich Passwörter, die ich mir merken kann?
Es MUSS für jeden Account ein eigenes Passwort bestehen!

Warum sichere Passwörter wichtig sind
Passwörter schützen deine **persönlichen Daten**, Konten und oft auch dein Geld.
Schwache Passwörter können leicht durch:
Brute-Force-Angriffe (systematisches Ausprobieren),
Wörterbuchangriffe (häufige Wörter & Kombinationen),
Datenlecks (wiederverwendete Passwörter)
geknackt werden.
Ein einziges kompromittiertes (nicht mehr sicher / in fremde Hände geraten / manipuliert) Passwort kann mehrere Konten gefährden.
Wenn man sagt: „Ein kompromittiertes Passwort“ heißt das:
Es ist **nicht mehr geheim**
Es sollte **sofort geändert** werden
Alle Konten mit demselben Passwort sind **gefährdet**

Wie man sichere Passwörter erstellt
1. Lang ist wichtiger als kompliziert

Mindestens **12–16 Zeichen**, je länger desto besser
Länge erhöht die Sicherheit stärker als Sonderzeichen allein
❌ Pa$$w0rd
✅ Giraffe-trinkt-Kaffee-2025!

2. Eine Passphrase statt eines Wortes
Kombiniere mehrere **zufällige Wörter -** Leicht zu merken, schwer zu knacken
Beispiel:
Mond!Apfel7Regenstuhl

3. Mischung aus Zeichen
Verwende:
Groß- und Kleinbuchstaben
Zahlen
Sonderzeichen (! ? % # @)
Aber: **nicht vorhersehbar** (z. B. kein Passwort123!)

4. Keine persönlichen Infos
Vermeide: Namen, Geburtstage, Haustiere, Benutzernamen oder E-Mail-Adressen
Diese Infos sind oft öffentlich oder leicht zu erraten.

5. Jedes Konto ein eigenes Passwort
Nie dasselbe Passwort mehrfach verwenden, Sonst reicht ein einziges Datenleck für alle Konten

6. Passwort-Manager nutzen (sehr empfohlen)
Erstellen & speichern extrem starke Passwörter
Du musst dir nur **ein Master-Passwort** merken
Bekannte Beispiele: Bitwarden, 1Password, KeePass

7. Zwei-Faktor-Authentifizierung (2FA) aktivieren
Zusätzliche Sicherheit (z. B. App oder SMS)
Selbst bei Passwortdiebstahl bleibt dein Konto geschützt

Merksatz
Ein gutes Passwort ist lang, einzigartig und zufällig – und idealerweise vom Passwort-Manager erstellt.

Phishing

Nach Daten angeln

- 🎣 **Gefälschte Absender:** E-Mails sehen aus, als kämen sie von Banken, Online-Shops oder Behörden.
- ⚠️ **Dringlichkeit:** „Ihr Konto wird gesperrt, wenn Sie nicht sofort reagieren!“
- 🔗 **Manipulierte Links**: Sie führen auf täuschend echt aussehende Webseiten, die Daten abfangen.
- 📩 **Anhänge:** Oft mit Schadsoftware versehen.

16.12.2025 Christiane Stadtfeld - Anita Velten 4

Phishing ist eine Form von Cyberkriminalität, bei der Angreifer versuchen, Menschen durch gefälschte Nachrichten (oft E-Mails, SMS oder Webseiten) dazu zu bringen, vertrauliche Informationen preiszugeben – zum Beispiel Passwörter, Kreditkartendaten oder Bankzugänge. Der Begriff kommt vom englischen „fishing“ (Angeln), weil die Täter quasi „nach Daten angeln“. Typische Merkmale sind:
- 🎣 Gefälschte Absender: E-Mails sehen aus, als kämen sie von Banken, Online-Shops oder Behörden.
- ⚠️ Dringlichkeit: „Ihr Konto wird gesperrt, wenn Sie nicht sofort reagieren!“
- 🔗 Manipulierte Links: Sie führen auf täuschend echt aussehende Webseiten, die Daten abfangen.
- 📩 Anhänge: Oft mit Schadsoftware versehen.

Phishing (Angeln nach Daten)
Dabei senden Kriminelle gefälschte E-Mails oder Nachrichten, die wie offizielle Mitteilungen von Banken, Dienstleistern oder anderen vertrauenswürdigen Quellen aussehen.

Oft werden die Opfer dabei sogar persönlich angesprochen/angeschrieben, was

den Erfolg dieser Methode ausmacht. **Man soll dazu verleitet werden, sensible Daten preiszugeben**, etwa Passwörter für Internetseiten oder zum Beispiel Kreditkartendaten. Dabei wird alles so gut getarnt und getäuscht, dass man oft gar nicht bemerkt, wie man selbsttätig die eigenen Daten preisgibt und eintippt.

Weil solche Phishing-Nachrichten keinen Virus enthalten, bleibt ein Virenscanner oft wirkungslos. Man sollte **Links in E-Mails stets hinterfragen** und im Zweifelsfall nicht anklicken. Statt einem Virenscanner hilft hier eher der Spam-Filter im E-Mailprogramm, doch auch dieser erkennt die gefälschten Mails nicht immer. Die beste Waffe gegen diese **psychologischen Betrugsmethoden** sind also keine Schutzprogramme, Spam-Filter oder Virenscanner, sondern **der menschliche Verstand**.

Social Engineering (soziale Manupilation) – Vertrauen ausnutzen
Beim sogenannten Social Engineering manipulieren Angreifer ebenfalls unmittelbar auf psychologischer Ebene den Menschen und nicht auf technischer Ebene den Computer.

Man könnte es auch mit sozialer Manipulation übersetzen. Dies kann telefonisch, per Chat, SMS oder sogar persönlich geschehen. Ein häufiger Trick ist es, dass die Betrüger sich als Mitarbeiter einer bekannten Firma oder als IT-Support ausgeben, um an sensible Informationen wie Passwörter oder Zugangsrechte zu kommen. Auch hier ist ein Virenscanner machtlos, da der Angreifer keine Schadsoftware nutzt und nicht auf technischer Ebene agiert.

Um sich zu schützen, ist es wichtig, generell erstmal keine vertraulichen Informationen herauszugeben und solche Anfragen immer kritisch zu hinterfragen. In solchen Fällen nehmen sich die Betrüger oft viel Zeit, um Vertrauen aufzubauen. Es wird ein Gespräch geführt, in dem es anfangs vielleicht auch erstmal um ganz andere Dinge geht, bevor dann irgendwann der Betrug eingeleitet wird. Man kennt dieses Verfahren aus der “analogen nicht digitalen Vergangenheit” zum Beispiel von Heiratsschwindlern oder auch vom Enkeltrick. Diese Methoden werden mittlerweile auch angewendet, um an Passwörter oder andere Zugangsdaten zu kommen oder eine freiwillige Zahlung an die Betrüger zu veranlassen.

Account Takeover – Die Übernahme von Benutzerkonten
Beim sogenannten “Account Takeover” nutzen Angreifer gestohlene oder schwache Zugangsdaten (schlechte Passwörter mit wenigen Stellen, keinen Zahlen und Ziffern), um sich in fremde Online-Konten einzuloggen, etwa auf sozialen Netzwerken, bei Online-Shops oder bei E-Mail-Diensten. Die Zugangsdaten stammen oft aus großen Datenlecks oder werden sogar

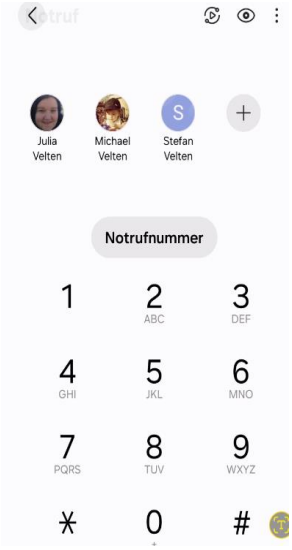
manchmal durch Ausprobieren erraten, wenn Nutzer zu einfache Passwörter verwenden. Da auch hierbei keine Schadsoftware auf dem Gerät des Opfers installiert wird, hat auch in diesem Fall ein Virenscanner keine Chance, diesen Angriff zu bemerken.

Notfall – Notruf – eingerichtet?

Notfall-Informationen hinterlegen

Notfallkontakt anrufen, ohne das Handy zu entsperren

Notfall oder Notruf tippen



17.12.2025 Christiane Stadtfeld - Anita Velten 5

Handy: Notfall-Informationen hinterlegen
Es können Situationen eintreten, in denen es sehr wichtig sein kann, dass andere Menschen schnell etwas über uns erfahren, das wir momentan nicht zu äußern in der Lage sind - sozusagen ohnmächtig.
Ersthelfer im Notfall sollten wissen, wen sie benachrichtigen sollen, wenn wir es nicht können. Für Rettungssanitäter oder Ärzte ist es wichtig, über Allergien, Vorerkrankungen, wichtige Medikamente o.ä. zu erfahren.
Sowohl Android-Geräte als auch das iPhone bieten deshalb die Möglichkeit, Notfallinformationen und Notfallkontakte zu hinterlegen und diese Informationen direkt auf dem Sperrbildschirm anzuzeigen.
So können Rettungskräfte oder Ersthelfer bei einem Unfall wichtige Daten sehen, ohne das Handy entsperren zu müssen. Es ist sogar möglich, auf diese Weise die hinterlegten Notfallkontakte anzurufen, **ohne das Handy zu entsperren.**
Und was noch geht: Stell dir vor, du hast dein Handy verloren. Dann kann der ehrliche Finder deinen Notfallkontakt anrufen - wenn er weiß, wie es geht.

Weihnachselfen

- ElfYourself - The #1 Holiday App of All Time!

- https://elfyourself.com?mld=1105615