DSGVO und Awareness gegen Hackingangriffe

Datenschutz

Webex, Juni 2022, Montanuniversität Leoben

UNTERNEHMENSGRUPPE

Vorstellung

Mag. iur. Martina Wenghofer MA

Datenschutzjuristin

bei x-tention Informationstechnologie GmbH

Ausbildung

Studium der Rechtswissenschaften

Studium IT-Recht und Management

Zertifizierungen

Datenschutzbeauftragter (WIFI - Wirtschaftsförderungsinstitut)

Mag. iur. Tina Nagler

Datenschutzjuristin

bei x-tention Informationstechnologie in Graz

Ausbildung

Studium der Rechtswissenschaften

Zertifizierungen

Datenschutzbeauftragte (Bitkom Akademie)

Agenda

01 Hackerangriffe

02 Social Engineering

03 Sicherheit von E-Mails

04 Passwörter

05 Clean Desk

06 Lessons Learned

07 Zeit für Fragen

01

Hackerangriffe

Kurze Einführung und Beispiele

Aktuelle Fälle

Beispiele:

CYBERANGRIFF

Hackerangriff in Kärnten: Veröffentlichte Daten sind wohl echt

Landessprecher Kurath: "Gehen davon aus, dass veröffentlichte Daten mit den Daten des Landes übereinstimmen"

7. Juni 2022, 15:04, 24 Postings

Cyberangriff auf die Medizinische Universität Innsbruck

Hackerangriff auf Medizin-Uni Innsbruck

von ANDREAS TRÖSCHER

Zweite Attacke innerhalb von einem Monat auf eine institutionelle Einrichtung in Österreich. Internetkriminalität nimmt ständig zu.

Gestohlene Daten sind online, Land kann sie aber nicht sichern

Die Hacker haben erneut Daten veröffentlicht, die aus dem Cyberangriff auf die Kärntner Landesverwaltung Ende Mai stammen. Land Kärnten tappt im Darknet im Dunkeln.

Tiroler Polizei ermittelt nach Hacker-Angriff auf Innsbrucker Meduni

Details werden aus "ermittlungstaktischen Gründen" nicht bekanntgegeben.

Einführung

Definitionen

Was ist Hacking?

- Aktivitäten, bei denen versucht wird, digitale Geräte wie Rechner, Smartphones, Tablets oder ganze Netzwerke zu kompromittieren.

Was sind Gründe für Hackergangriffe?

- Finanzielle Motive (Bereicherung)
- Image innerhalb der Hackerszene
- Wirtschaftliche Motive (Betriebsspionage)
- Politische Motive

Welche Arten von Hackern gibt es?

- White-Hat-Hacker: „gute Hacker“, deren Ziel es ist, Sicherheitssystemen zu verbessern
- Black-Hat-Hacker: „böse Hacker“, die durch kriminelle Aktivitäten Schaden erzeugen möchten
- Grey-Hat-Hacker: „ein bisschen was von beiden Hacker“, die in Systeme eindringen ohne kriminellen Schaden zu erzeugen und dem Betroffenen die Schwachstellen aufzeigen und gegen Geld beseitigen

Wert der Daten

1. Individuelle Bewertung

- Zahlungsbereitschaft, um Daten zu schützen
- Bereitschaft, Daten gegen Geld zu verkaufen

2. Marktbewertung

- Unternehmensgewinn pro Datensatz
- Kosten eines Datenleaks
- regulärer Marktpreis für Daten
- Schwarzmarktpreis für Daten

3. Schwarzmarktwert von personenbezogenen Daten

- FBI: 50 US-$/Datensatz
- PhishLabs (Cybercrime-Abwehr): 10 US-$/Datensatz
- Beazley ("Cyber-Versicherer"): 40 bis 50 $/Datensatz
- Ransomware: meist 200 bis 300 $/Datensatz pro Attacke, aber bis zu mehreren Millionen in gezielten Attacken
- Im Fall Land Kärnten: 5 Mio. US-$ in Bitcoin

02

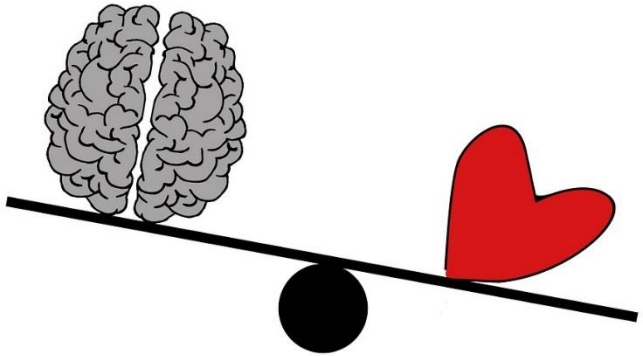
Social Engineering

Mitarbeiter als Angriffsziel

Was ist Social Engineering?

Ausnutzen **menschlicher Eigenschaften**, um an Informationen zu kommen

Hilfsbereitschaft
Kundenfreundlichkeit
Dankbarkeit
Gutgläubigkeit
Respekt vor Autoritäten
Konfliktvermeidung
Wunsch, guter Teamplayer zu sein



Effiziente Methode zur Informationsbeschaffung meist ohne Einsatz technischer Hilfsmittel

Häufig die einfachste Form des Angriffs

Psychologie steht im Vordergrund

Meist zur Vorbereitung für einen Hackerangriff

Beispiele aus der Praxis

Anruf vom „Administrator“ (z.B. Microsoft-Mitarbeiter)

Verlangt Informationen über bestimmte Systeme

… oder Auskunft über Passwort

Gefundener USB-Stick am Parkplatz

Wird bewusst ausgelegt

Infiziert mit Schadsoftware

Aufhalten bzw. Aufsperren von zutrittsgesicherten Türen (z.B. Lieferant, Techniker)

Hilfsbereitschaft

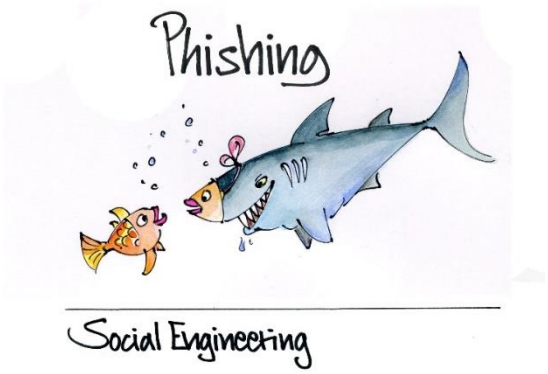
Leerstehende Büros mit offenen Türen

Gespräch im Freundeskreis (Wirtshaus etc.)

Weitererzählen von Infos über Patienten, neue Technologien usw.

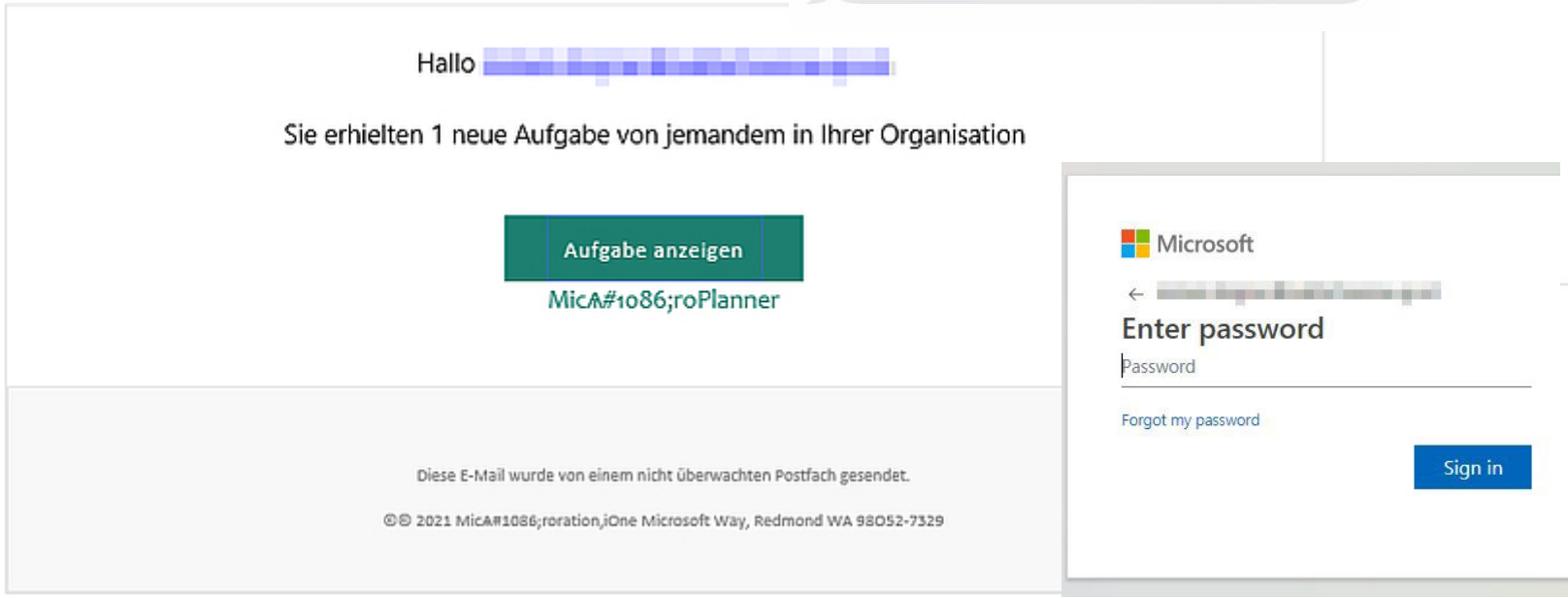
CEO Fraud

E-Mail vom „Chef“ zum Überweisen von hohen Geldbeträgen



Quelle: https://www.presseportal.de/pm/58214/2885887

Beispiele aus der Praxis



Beispiele aus der Praxis

Von: Michael [mailto:replies24@yandex.com]
Gesendet: Freitag, 13. Oktober 2017 08:38
An:
Betreff: kontostand

Guten Morgen,

Was ist unser Kontostand? Können wir heute 68T zahlen?

Gruß
Michael

---------- Weitergeleitete Nachricht ----------
Von: **Jürg Stuker** <pvtmail28@comcast.net>
Datum: 12. September 2016 um 11:39
Betreff: Bank Überweisung
An: @namics.com

Hallo Andreas,

Ich brauch dich um eine Überweisung nach England zu machen . sag mir welche Details du dafür brauchst ich werde sie dir umgehen zukommen lassen

Grüsse,

Jürg Stuker

Schutz vor Social Engineering

Hausverstand nutzen!

Würde mein Chef am Telefon wirklich verlangen, dass ich ihm mein Passwort weitergebe?

Warum ruft mich jemand an, der von mir wissen möchte, welche Schlüssel / Zutrittskarten / Betriebssysteme / Programme wir verwenden?

Seien Sie skeptisch gegenüber Fragen Unbekannter!

Rückruf verlangen!

Rufen Sie den Anrufer auf die im System hinterlegte bzw. die Ihnen bekannte Nummer zurück

Passwörter niemals weitergeben!

z.B. PINs, TANs, Passwörter

Sprechen Sie unbekannte Personen in sensiblen Bereichen an!

Schauen Sie mal rein …

Watchlist Internet
Internet-Betrug, Fallen & Fakes im Blick

Warnungen | Unseriöse Webseiten | Falle melden | Themen | Beratung & Hilfe | Videos

Neues Phishing-E-Mail der Erste Bank und Sparkasse

Themen: Datenklau, Geldtransfer, E-Mail, Spam, Bank, Phishing

Aktuell kursiert ein neues Phishing-E-Mail im Namen der Erste Bank und Sparkasse. Im Schreiben werden Sie über eine angebliche Abbuchung von 1 259 Euro informiert. Wenn Sie diese Zahlung nicht getätigt haben, sollten Sie auf einen Link klicken, um das Rückerstattungsverfahren einzuleiten. Achtung: Dieses E-Mail ist Fake und stammt nicht von der Sparkasse. Klicken Sie nicht auf den Link!

weiterlesen

03

Sicherheit von E-Mails

Wie erkenne ich Spam- und Phishing-Mails?

Was ist Phishing?

Ein Angreifer versucht, über …

gefälschte Webseiten,

gefälschte E-Mails oder

gefälschte Nachrichten

… an persönliche Daten zu gelangen (Identitätsdiebstahl)

Mögliche Folgen

Kontoplünderung

Datenverschlüsselung

Datenzerstörung

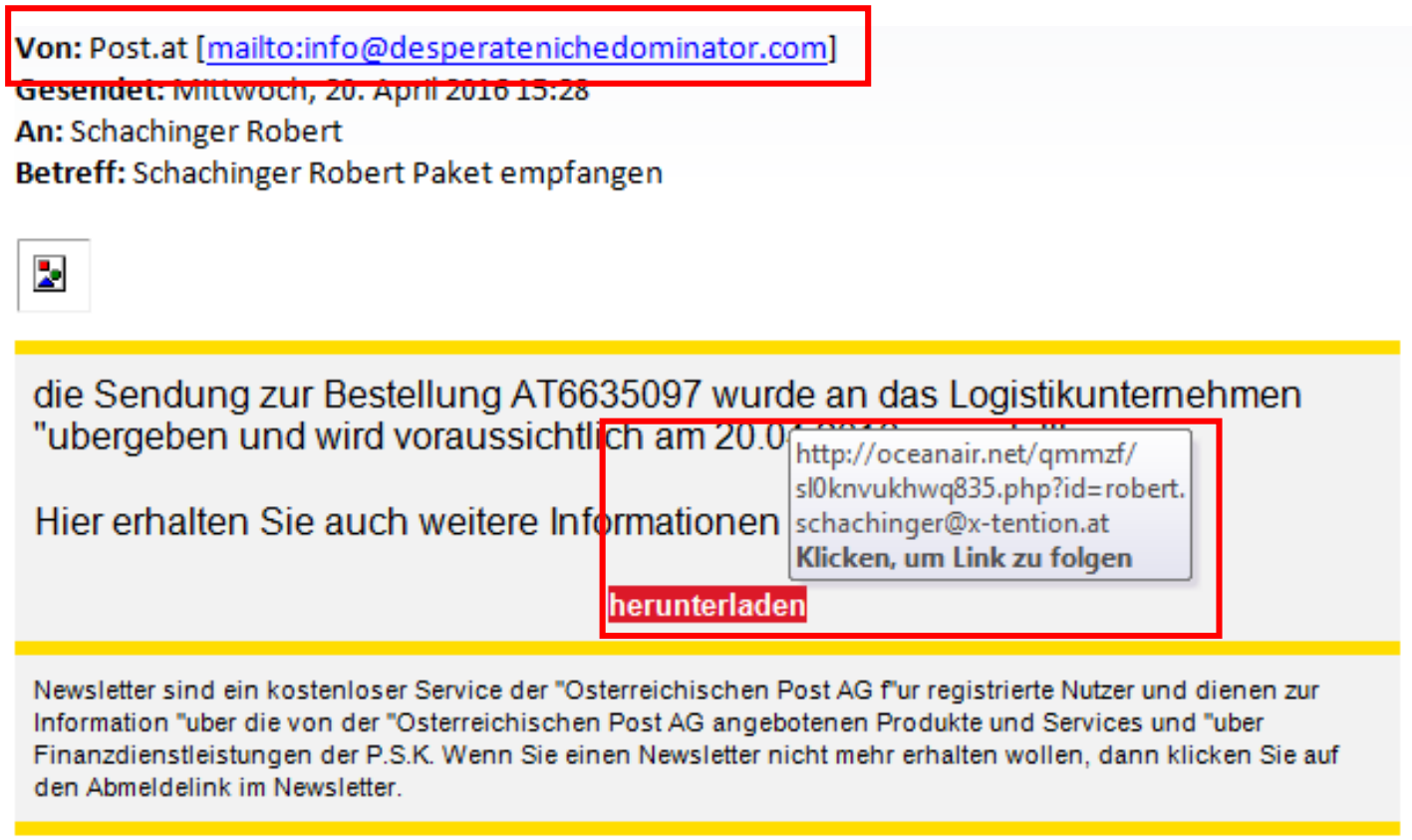
Erpressung

usw.

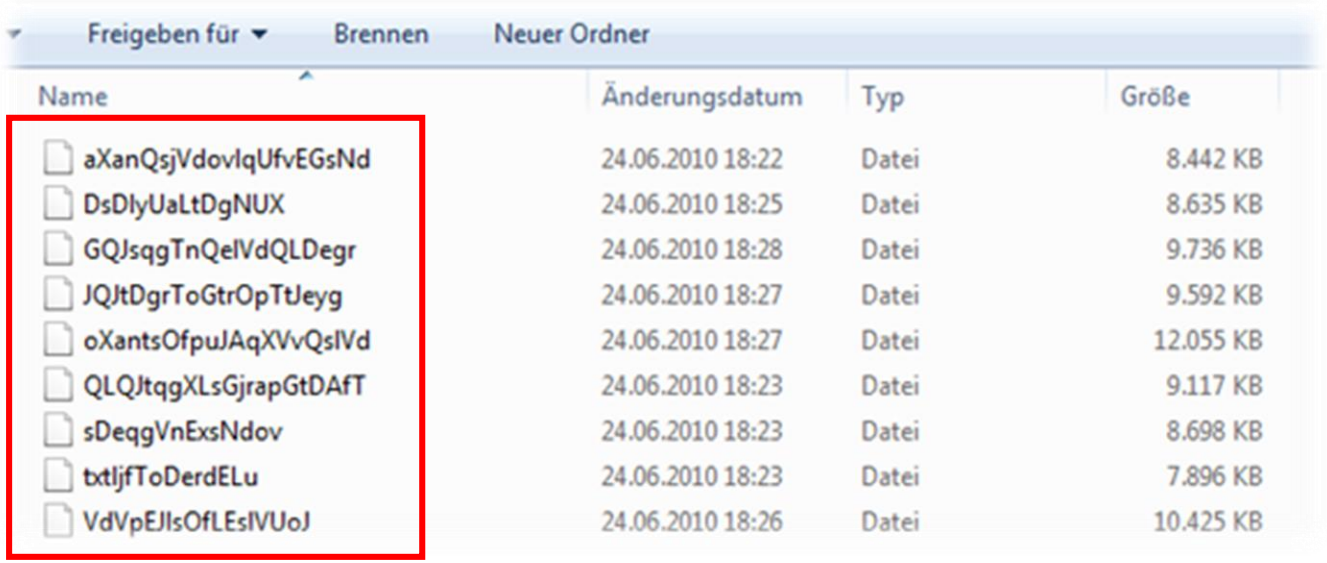
Bildquelle: pixabay.com

Wie kann ich mich schützen?

- E-Mails aufmerksam lesen (Rechtschreib- und Tippfehler)
- Kritisch hinterfragen, warum Sie bestimmte Mails bekommen
- Werden sensible Informationen abgefragt (z.B. PIN, Kontonummer)
- Absender-Adresse der E-Mail prüfen
- ACHTUNG: Angezeigter Namen ≠ Tatsächlicher Absender
- Link-Adresse im Mail kontrollieren
- ACHTUNG: Nur mit der Maus über den Link fahren, NICHT anklicken!
- Unbekannte Anhänge NICHT öffnen (z.B. Rechnungen)
- Siehe auch: www.watchlist-internet.at



Und wenn‘s doch passiert?



Vertrauensperson aus der IT und aus dem Datenschutz umgehend informieren!

DSGVO

Ansprechpartner bei Datenschutzangelegenheiten

Datenschutz-Koordinator

- Interne Ansprechperson für Datenschutz
- Anlaufstelle für Betroffenenrechte und Datenpannen
- Regelmäßige Aktualisierung und Verbesserung des Datenschutz-Managementsystems

Dr. Klaus Sapetschnig

+43 3842/402-7002

dsb@unileoben.ac.at

Datenschutzbeauftragter

- Unterrichtet und berät zum Thema Datenschutz
- Überwachung der Einhaltung Datenschutzvorschriften
- Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter
- Zentrale Anlaufstelle für die Datenschutzbehörde

Fa. x-tention Informationstrechnologie GmbH

Service.Datenschutz@x-tention.at

DSGVO

Data Breach / Datenschutzverletzung

Definition

- Datenschutzverletzung: Verletzung des Schutzes personenbezogener Daten.
- Identifizierte Datenschutzverletzungen sind unverzüglich weiterzuleiten!
- Meldung innerhalb von 72 Stunden an die Datenschutzbehörde, wenn ein Risiko für betroffene Person besteht.

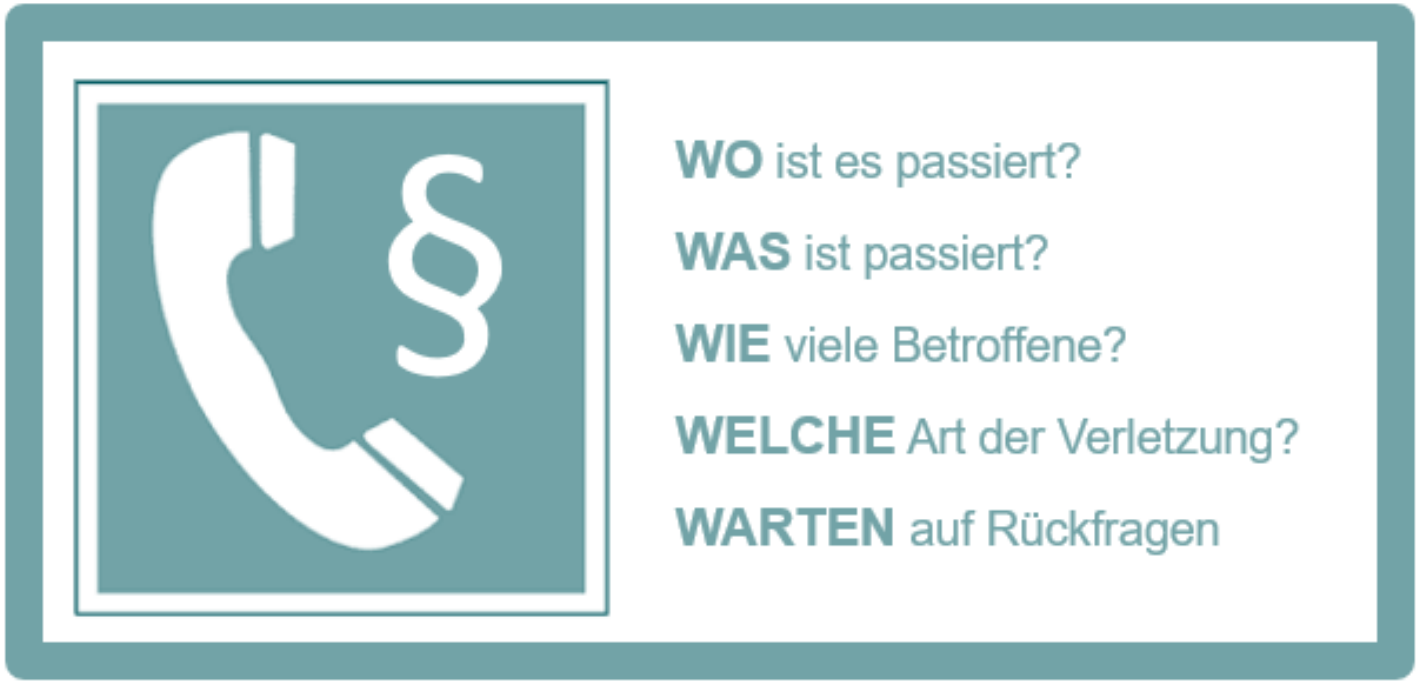
Beispiele für Datenschutzverletzungen

- Ungewünschte Veröffentlichung von personenbezogenen Daten im Internet
- Versehentliches Versenden von personenbezogenen Daten an falsche Empfänger
- Verlust oder Diebstahl von Datenträgern
- Weitergabe personenbezogener Daten an unbefugte Dritte

Datenschutzvorfälle

Was ist wichtig?

Welche Informationen sind zu melden?



04

Passwörter

12345678; Pa$$word; Passwort123…

Warum soll ein Passwort sicher sein?

- Dritte sollen nicht in Ihrem Namen arbeiten
  - Zugriff auf Daten (Studierendendaten)
  - Setzen von Aktivitäten (z.B. Löschen / Ändern von Dateien)
  - Es ist nachvollziehbar, was Ihr User macht, den Sie verantworten
- Zugriff auf Ihr E-Mail-Konto
  - Senden von E-Mails in Ihrem Namen
  - Zurücksetzen der Passwörter für Ihre Accounts im Internet
- Einkaufen auf Ihre Rechnung
  - Amazon, eBay usw.

Ein sicheres Passwort ist daher in Ihrem Interesse!

Gibt es überhaupt ein „sicheres“ Passwort?

- Anforderungen an „sichere“ Passwörter
  - Mindestlänge: 16 Zeichen
  - Komplexität (Kombination aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen)
  - Regelmäßiges Ändern der Passwörter
  - Passworthistorie
  - Vermeidung von Privatbezug (z.B. Geburtstag)
  - Vermeidung von Wörtern aus Wörterbüchern
  - Trennung zwischen Privat- und Firmenpasswörtern
  - Unterschiedliche Passwörter je Applikation (vor allem im Internet problematisch) usw.

- Fazit
  - Anforderungen an sichere Passwörter sind nicht praxistauglich!
  - Umgang mit Passwörtern ist in der Regel unsicher!

Ich brauche aber Passwörter, was also tun?

- Praxistaugliche Anforderungen an sichere Passwörter
  - Mindestlänge: 10-12 Zeichen
  - Komplexität (Kombination aus Groß-, Kleinbuchstaben, Ziffern und Sonderzeichen)
  - Ändern der Passwörter jährlich

- Verwenden Sie 3 sichere Passwörter:
  - 1 sicheres Passwort für Unternehmen
  - 1 sicheres Passwort für Privatgebrauch (z.B. Amazon)
  - 1 sicheres Passwort für **E-Mail-Account**
  - 1 Passwort für „Unwichtiges“ im Internet (z.B. Gewinnspiele)

Fazit: Lieber weniger Passwörter, dafür aber sichere!

Wie komme ich zu einem sicheren und einfache zu merkenden Passwort?

- Verwenden Sie Merkhilfen
  - z.B. Ich fahre gerne jeden 2. Sonntag mit meinem Oldtimer!

  - Passwort: Ifgj2SmmO!

Home Notify me Domain search Who's been pwned **Passwords** API About Donate

Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. Read more about how HIBP protects the privacy of searched passwords.

password **pwned?**

Generate secure, unique passwords for every account **Learn more at 1Password.com**

Why 1Password?

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

05

Clean Desk

Sicherer Umgang mit Datenträgern

Was ist beim Clean Desk zu beachten?

- Sie sind für Ihren Arbeitsplatz verantwortlich
- Sperren Sie Ihren Bildschirm, sobald dieser außerhalb Ihres Sichtfeldes ist Windows -Taste + „L“
- Lassen sie Dokumente mit personenbezogenen Daten nicht unbeaufsichtigt, offen auf Ihrem Arbeitsplatz liegen
- Ausgedruckte Dokumente dürfen nicht im Drucker verbleiben
- Vertrauliche Dokumente und Informationsträger (z.B. USB-Sticks) sind vor längeren Abwesenheiten (abends, vor Urlauben) zu verschließen
- Nicht mehr benötigte vertrauliche Dokumente/Datenträger sind sicher zu vernichten (Shredder, Entsorgung durch ZID bei Datenträgern)

06

Lessons Learned

Was gibt’s zu merken?

1. Datenschutz ist wichtig
2. Hausverstand benutzen und Situationen/E-Mails kritisch hinterfragen
3. Passwörter nie weitergeben
4. Daten haben einen Wert
5. Sie sind für Ihren Arbeitsplatz verantwortlich
6. Personenbezogene Daten dürfen nie im Hausmüll entsorgt werden
7. Nützliche Links:
   - https://haveibeenpwned.com/
   - https://www.watchlist-internet.at/

Zeit für Fragen ☺

Vorab eingesendete Frage

Dürfen COVID19-Daten an Mitarbeiter*innen weitergegeben werden? Z. B. wer am Lehrstuhl an COVID19 erkrankt bzw. in Quarantäne ist.

- Daten über Infektionen sowie über Verdachtsfälle zählen zu jenen sensiblen Daten, für die das Datenschutzrecht einen besonderen Schutz vorsieht.

- Gleichzeitig sieht das Datenschutzrecht aber vor, dass Daten über den Gesundheitszustand in jenem Ausmaß verwendet werden können, das notwendig ist, um die Verbreitung des Virus einzudämmen und um die Mitmenschen zu schützen.

- Im Sinne des Grundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO ist daher im Einzelfall sorgfältig abzuwägen, ob es notwendig ist, den konkreten Namen einzelner Personen zu nennen, die sich infiziert haben, oder mit der allgemeinen Information, dass am Arbeitsplatz eine Infektion aufgetreten ist, das Auslangen gefunden werden kann.

- Eine individuelle Nennung von infizierten Personen kann sich dann als zulässig erweisen, wenn erhoben werden muss, wer mit diesen Personen vor Bekanntwerden der Infektion Kontakt hatte.

Regelung der Montanuniversität

- Im Rahmen des Contact Tracing werden nach Eingang einer Meldung einer positiv Testung die Lehrstühle bzw. OEs aufgefordert, Personen, die mit der betroffenen Person in Kontakt waren zu nennen und diese über den Fall zu informieren.

- Corona-Daten, die auf der OE oder am Lehrstuhl gespeichert/aufbewahrt werden müssen spätestens nach einem Semester gelöscht werden

- Weitere Informationen zum Datenschutz und COVID 19

- https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html

Vielen Dank

x-tention Informationstechnologie GmbH
Römerstraße 80a, 4600 Wels, Austria
Service.Datenschutz@x-tention.com

IT with care.