DSGVO und der richtige Umgang mit personenbezogenen Daten in meinem Arbeitsbereich

Datenschutz

Webex, April 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 Datenschutz – Kurze Einführung

02 Social Engineering

03 Sicherheit von E-Mails

04 Gesunder Umgang mit Social Media

05 Passwörter

06 Veranstaltungswerbung

07 Clean Desk

08 Lessons Learned

01

Datenschutz

Kurze Einführung

Datenschutz

Was ist Datenschutz?

- Schutz der Privatsphäre
- Freiheit der Menschen, ihre Daten selbst zu bestimmen (informationelle Selbstbestimmung)

Welche Gesetze sind zu beachten?

- DSGVO
- DSG
- FOG
- Etc.

DSGVO

Welche Arten von Daten gibt es?

Personenbezogene Daten

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (z.B. Adresse, Telefonnummer).

Besondere Kategorien personenbezogener Daten („sensible Daten“)

- Rassische oder ethnische Herkunft
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse oder weltanschauliche Überzeugungen
- Genetische oder biometrische Daten
- Gesundheit
- Sexualleben oder sexuelle Orientierung

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

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

02

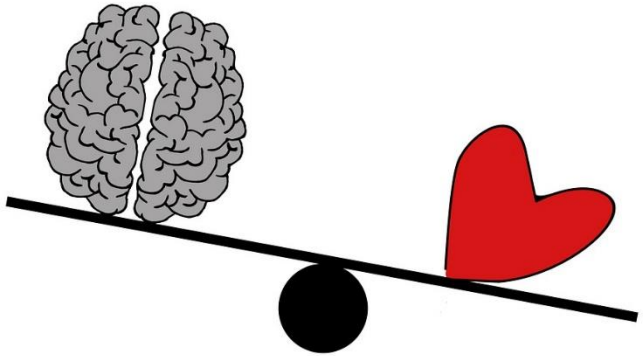
Social Engineering

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

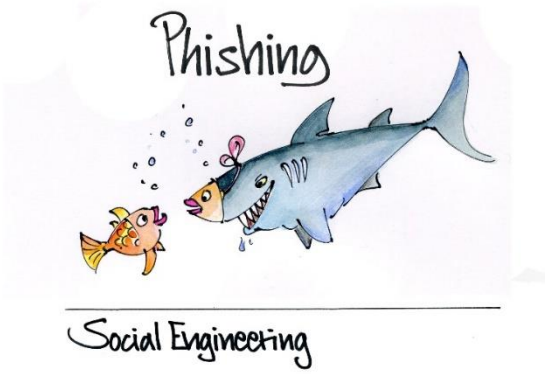
Leerstehende Büros mit offenen Türen

Gespräch im Freundeskreis (Wirtshaus etc.)

Weitererzählen von Infos über Patienten, neue Technologien usw.

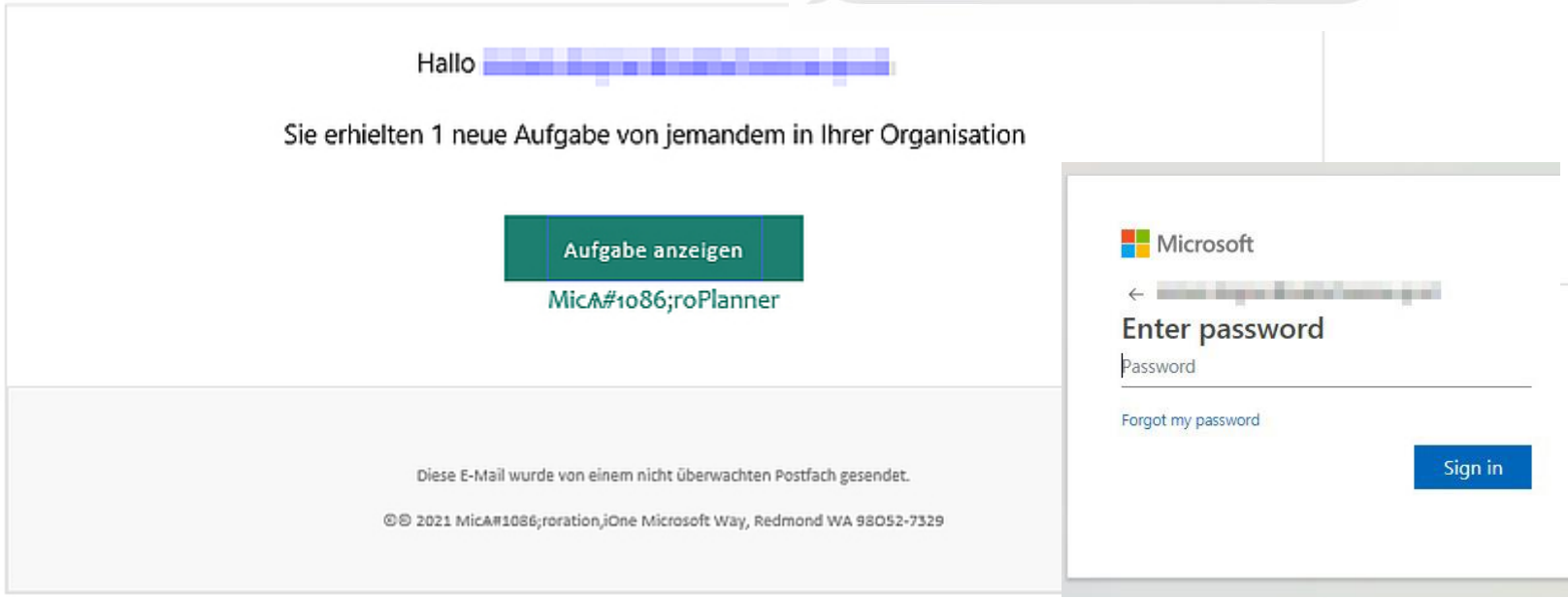
CEO Fraud

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



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

Beispiele aus der Praxis



Donnerstag, 1. Oktober 2020 Magenta®

📌 Unknown

Sehr geehrter Magenta-Kunde:

Herzliche Glückwünsche! Heute ist Ihr Glückstag!
Sie sind einer von 10 zufällig ausgewählten Benutzern, die die Chance haben, ein **Samsung Galaxy S20**, **iPhone 11 Pro** oder **MacBook Air** zu gewinnen.

OK

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

Beispiele aus der Praxis

Gespräch über Urlaub

Wohin geht es als nächstes in den Urlaub?

Waren Sie schon einmal dort?

Wann geht es denn los?

Wie lange bleiben Sie dort?

Wer kümmert sich um Ihr Haus / Ihre Wohnung?

Unterschätzen Sie nie den Wert einer Information!

Sie verraten dabei:

Ab wann Ihr Haus / Ihre Wohnung leer steht

Wie lange Sie nicht zu Hause sein werden

Ob regelmäßig jemand vorbeikommt

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!

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

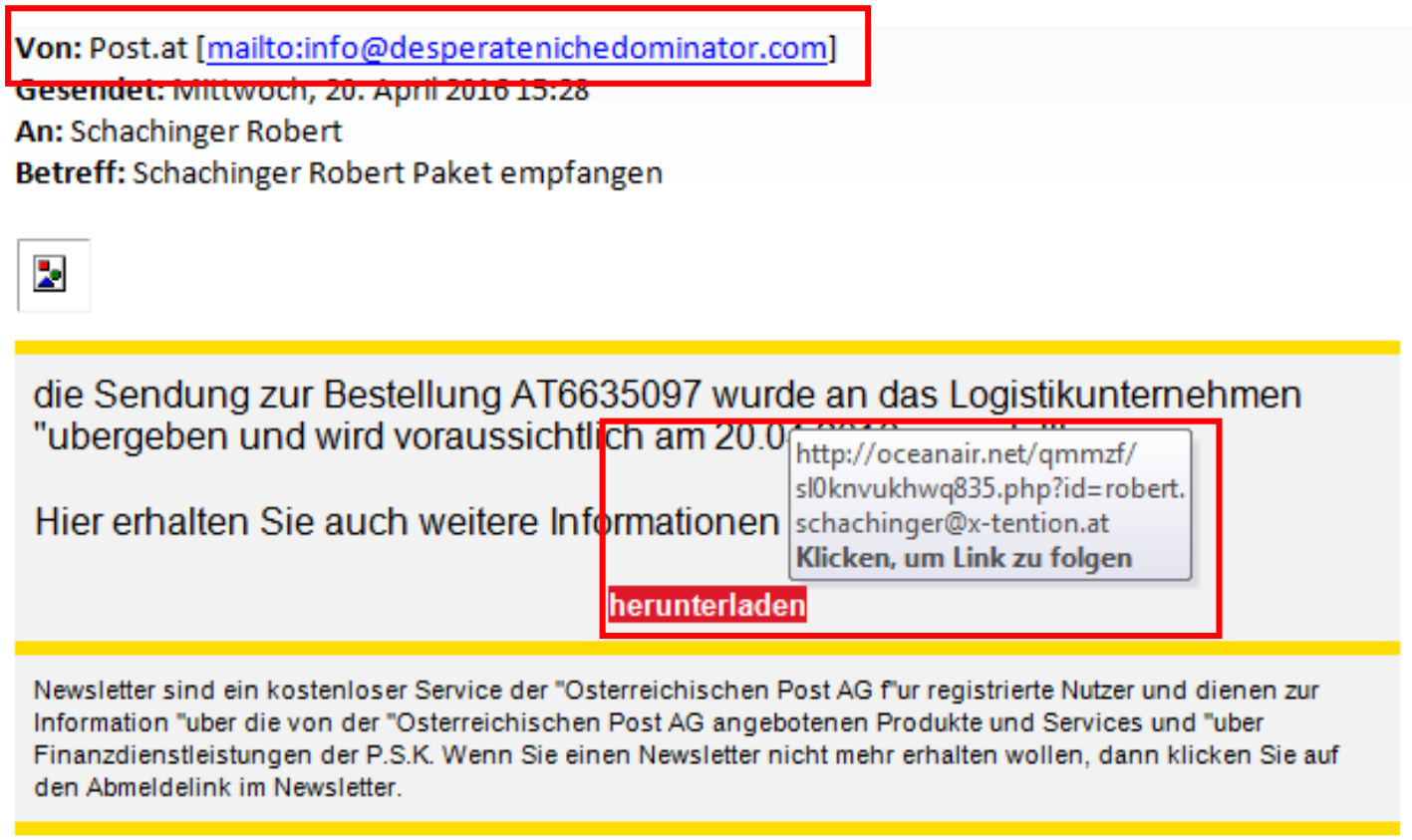
Erpressung

usw.

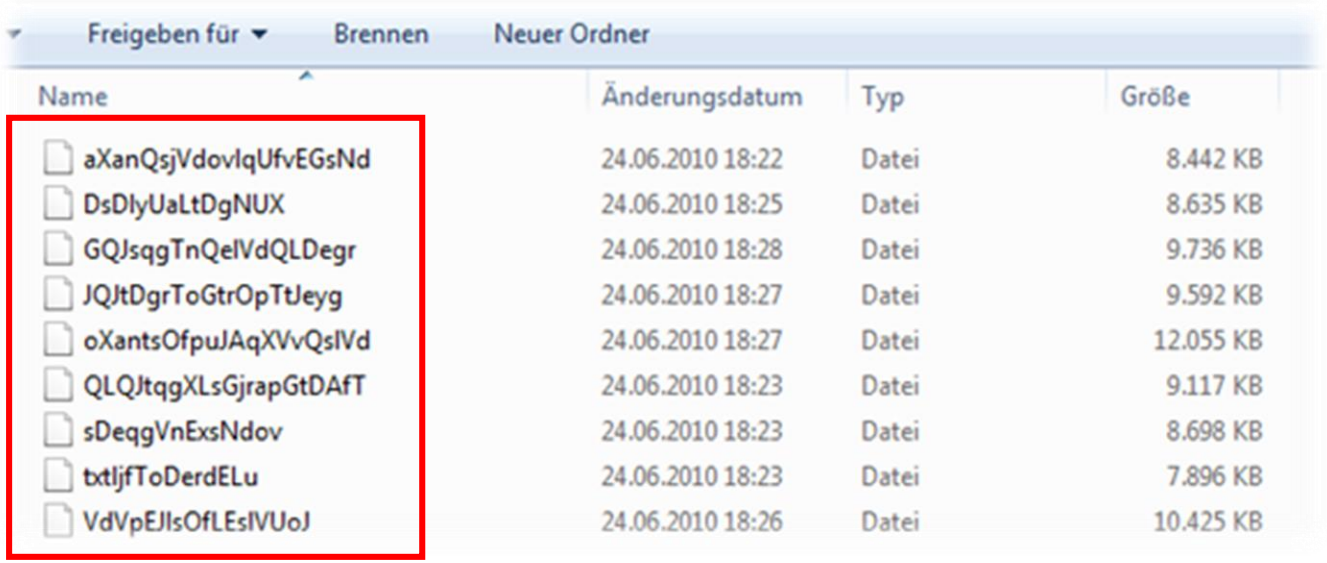
Bildquelle: pixabay.com

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 umgehend informieren!

04

Gesunder Umgang mit Social Media

Richtiger Umgang mit Social Media

Vertraulichkeit

Unispezifische Daten haben nichts in sozialen Medien verloren – Es gibt offizielle Social Media Auftritte der MUL.

Urheberrecht

Respektieren Sie stets das Urheberrecht

Posten Sie nur Inhalte, zu deren Veröffentlichung Sie auch befugt sind

Hausverstand benutzen!

Gut überlegen was man kommentiert, liket, postet oder repostet

Themen wie Arbeit, Kollegen etc. vermeiden – man weiß nie, wer z.B auf Facebook mitliest

Netiquette Einhalten

Keine rassistischen, sexistischen oder in einer anderen Art diskriminierenden Inhalte posten.

Zugangsdaten schützen!

Benutzername und Passwort nie weitergeben

Wer hat Interesse an meinen Daten?

Interessenten und Geschäftsmodelle mit Daten

Interessent:

- Konsum-Unternehmen
- Forscher
- Arbeitgeber
- Versicherungen
- Pharmaunternehmen
- Hacker

Geschäftsmodell:

- Gezielte Werbung
- Forschungsvorhaben
- Bewerbungen/Kündigungen
- Erhöhung von Preisen, Risikominimierung
- Forschung, Preismodelle
- Social Engineering Angriffe
- Identitätsdiebstahl
- Daten-Geiselnahme/Erpressung

HOME > KARRIERE > SOCIAL MEDIA: POSTS VERRATEN, WER HIGH UND LOW PERFORMER IST

Social Media: Forscher sagen aus Posts von Studierenden High und Low Performer vorher

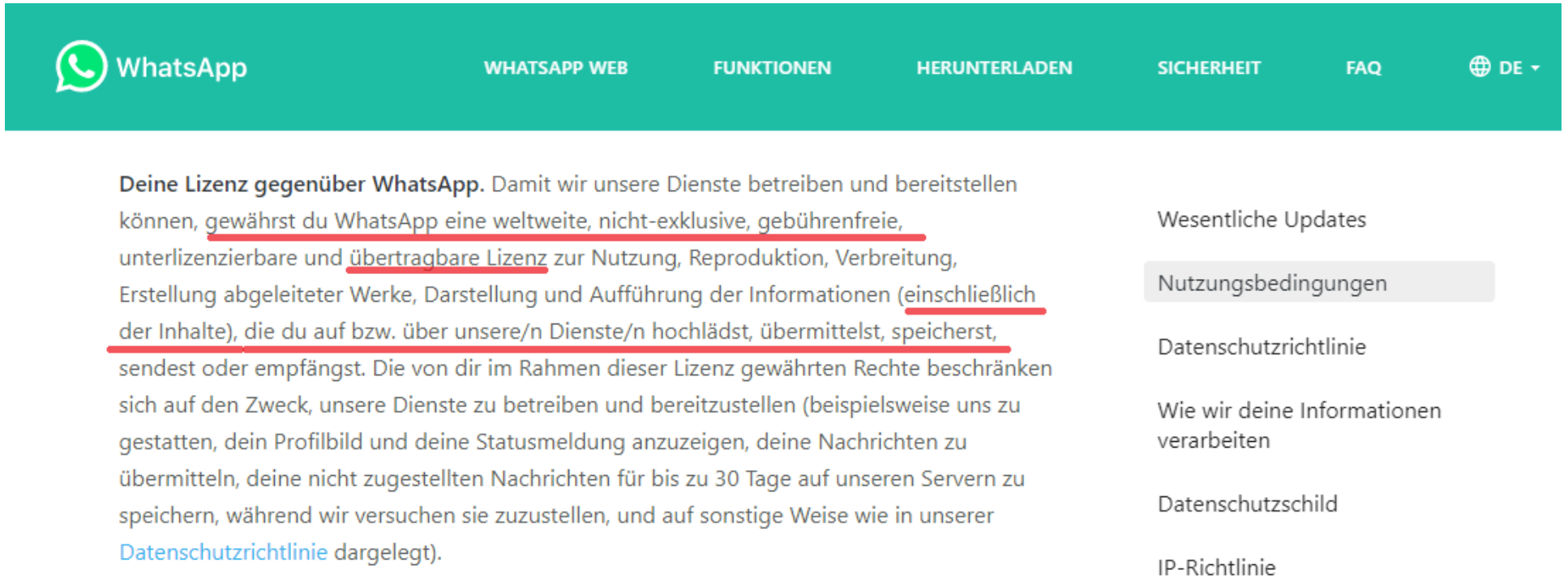
Nora Bednarzik
27 Okt 2020

Die Sprache auf sozialen Medien kann laut Forschern viel über den Bildungsstand verraten. © Photo by Westend61 via Getty Images

ANZEIGE

[Estimating educational outcomes from students' short texts on social media | EPJ Data Science | Full Text (springeropen.com)]

Insbesondere wenn du Inhalte, die durch geistige Eigentumsrechte geschützt sind, auf oder in Verbindung mit unseren Produkten teilst, postest oder hochlädst, räumst du uns eine nicht-ausschließliche, übertragbare, unterlizenzierbare, gebührenfreie und weltweite Lizenz ein, deine Inhalte (gemäß deinen Privatsphäre- und App- Einstellungen) zu hosten, zu nutzen, zu verbreiten, zu modifizieren, auszuführen, zu kopieren, öffentlich vorzuführen oder anzuzeigen, zu übersetzen und abgeleitete Werke davon zu erstellen. Das bedeutet beispielsweise, dass du uns, wenn du ein Foto auf Facebook teilst, die Berechtigung dazu gibst, es zu speichern, zu kopieren und mit anderen zu teilen (wiederum im Einklang mit deinen Einstellungen); dies können u. a. Dienstleister sein, die unseren Dienst oder andere von dir genutzte Facebook-Produkte unterstützen. Diese Lizenz endet, wenn dein Inhalt aus unseren Systemen gelöscht wird.


WhatsApp
WHATSAPP WEB
FUNKTIONEN
HERUNTERLADEN
SICHERHEIT
FAQ
DE
Deine Lizenz gegenüber WhatsApp. Damit wir unsere Dienste betreiben und bereitstellen können, gewährst du WhatsApp eine weltweite, nicht-exklusive, gebührenfreie, unterlizenzierbare und übertragbare Lizenz zur Nutzung, Reproduktion, Verbreitung, Erstellung abgeleiteter Werke, Darstellung und Aufführung der Informationen (einschließlich der Inhalte), die du auf bzw. über unsere/n Dienste/n hochlädst, übermittelst, speicherst, sendest oder empfängst. Die von dir im Rahmen dieser Lizenz gewährten Rechte beschränken sich auf den Zweck, unsere Dienste zu betreiben und bereitzustellen (beispielsweise uns zu gestatten, dein Profilbild und deine Statusmeldung anzuzeigen, deine Nachrichten zu übermitteln, deine nicht zugestellten Nachrichten für bis zu 30 Tage auf unseren Servern zu speichern, während wir versuchen sie zuzustellen, und auf sonstige Weise wie in unserer Datenschutzrichtlinie dargelegt).
Wesentliche Updates
Nutzungsbedingungen
Datenschutzrichtlinie
Wie wir deine Informationen verarbeiten
Datenschutzschild
IP-Richtlinie

05

Passwörter

12345678; Pa$$word; Passwort123…

Warum soll ein Passwort sicher sein?

- Dritte sollen nicht in Ihrem Namen arbeiten
  - Zugriff auf Daten (Bewohnerakte)
  - 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.

06

Veranstaltungswerbung

§174 Abs. 1 TKG

Darf man Informationsmails versenden?

grundsätzlich ja, aber Begriff der Werbung ist weit auszulegen.

- Werbung
  - §174 TKG Anrufe – einschließlich das Senden von Fernkopien (E-Mails) – zu Werbezwecken ohne vorherige Einwilligung des Nutzers sind unzulässig.
  - Sobald der Absender auch eigene wirtschaftliche Vorteile im Auge hat, dann handelt es sich um Werbung.
  - Eine Gestaltung der E-Mail als Newsletter oder Info-Mail hindert die Qualifikation als "Direktwerbung" nicht.

Kann ich einen Newsletter ohne Einwilligung schicken?

Ja ist möglich, wenn Folgende Voraussetzungen erfüllt sind:

- der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und
- diese Nachricht zur Direktwerbung für eigene ähnliche Produkte/Veranstaltungen oder Dienstleistungen erfolgt und
- der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und
- der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Ein-tragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.

07

Clean Desk

Sicherer Umgang mit Datenträgern und richtige Entsorgung

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)

08

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. Nutze Soziale Medien mit Bedacht
5. Elektronische Werbung ist nur unter bestimmten Voraussetzungen erlaubt
6. Personenbezogene Daten dürfen nie im Hausmüll entsorgt werden
7. Nützliche Links:
    - https://haveibeenpwned.com/
    - https://www.watchlist-internet.at/

Zeit für Fragen ☺

Vielen Dank

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

IT with care.