



Cyber Security Toolkit

Schutz vor Phishing, Sicherung von Unternehmensvermögenswerten und Erstellung robuster Passwörter



Phishing

Eine große Bedrohung für Unternehmen
auf der ganzen Welt





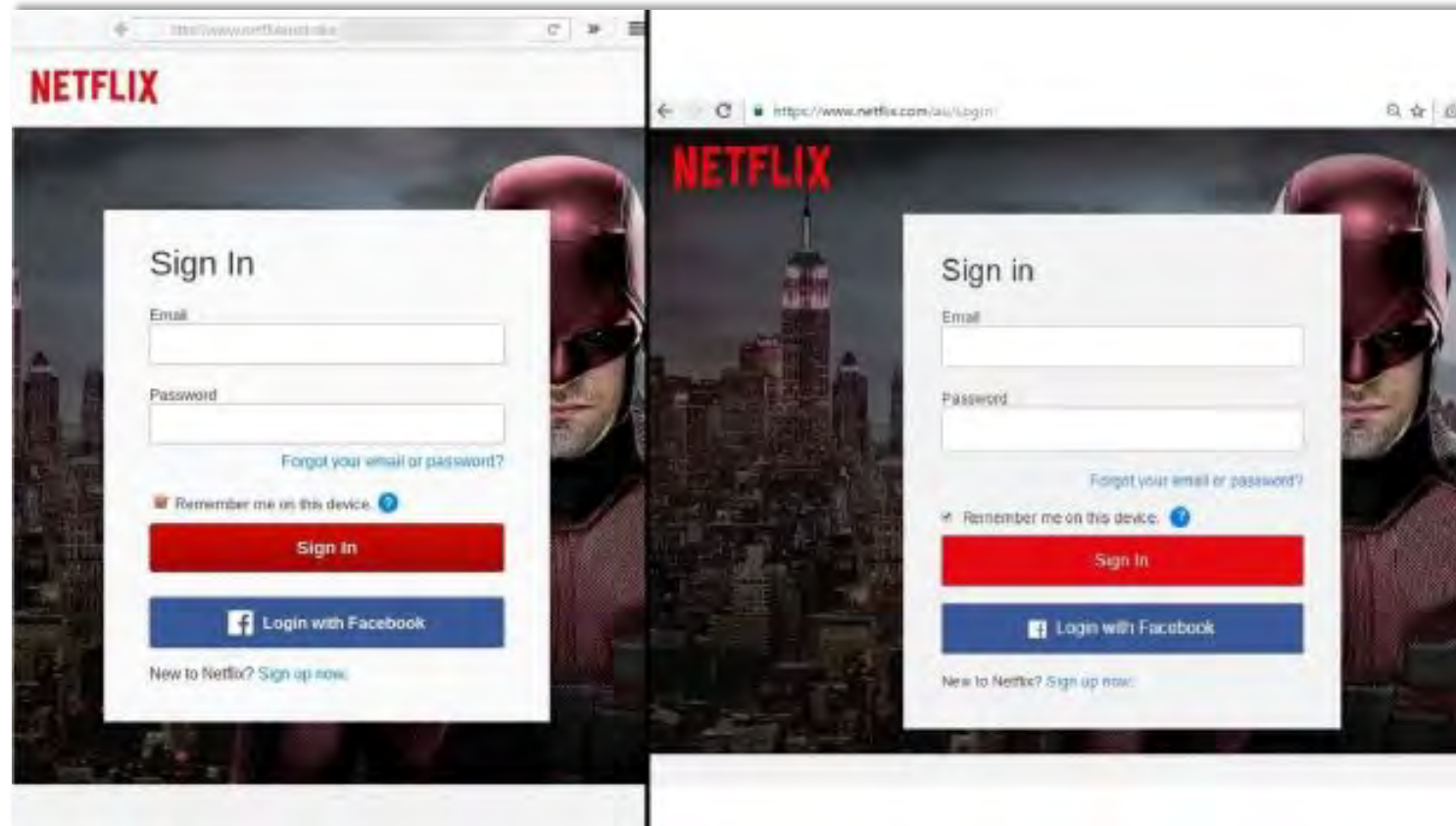
Was ist Phishing?

„Phishing ist ein krimineller Mechanismus, der sich sowohl Social Engineering als auch technischer Tricks bedient, um persönliche Daten und Zugangsdaten zu Bankkonten zu stehlen.“

- Die Gesamtanzahl der Phishing-Angriffe im Jahr 2016 belief sich auf **1.220.523**, was einen Anstieg von 65 % im Vergleich zum Jahr 2015 darstellt.
- Im Durchschnitt werden jeden Tag **190.000** neue Malware-Proben gefunden.



Phishing-Webseite: Welche ist gefälscht?



Bildquelle: <http://www.theage.com.au/business/consumer-affairs/phishing-emails-and-other-online-scams-on-the-rise-as-australians-lose-millions-of-dollars-20161115-gspnar.html>



Auswirkungen: Die Kosten einer Sicherheitsverletzung

48 % aller Sicherheitsverletzungen werden durch böartige oder kriminelle Angriffe verursacht.

Phishing-E-Mails führten von 2013 bis 2015 weltweit zu einem Gesamtverlust von mindestens **3,1 Milliarden US-Dollar**.



Die Arbeitsweise der Kriminellen

- Cyber-Kriminelle verwenden **Grafiken, korrekte Grammatik und Schlüsselsätze**, die denen der gefälschten Marke ähneln.
- Die Nachrichten, die sie versenden, **rufen Angst hervor** und drängen auf eine **sofortige Reaktion**.
- Cyber-Kriminelle **täuschen vor, eine Autoritätsperson** zu sein, um überzeugender zu wirken.

Phishing-Angriffe sind viel raffinierter, allgegenwärtiger und überzeugender, als wir meinen.

Beispiel für eine dringende E-Mail von einer Autoritätsperson



Bildquelle: <http://www.mailguard.com.au/blog/whaling-ceo-fraud-business-email-compromise-targeted-spear-phishing-attacks-continue-to-trouble-businesses>



Verschiedene Arten von Phishing: E-Mail-Phishing

Die derzeit größte Bedrohung für Unternehmen ist Phishing, einschließlich Spear-Phishing und betrügerischer CEO-E-Mails. Das sind E-Mail-Phishing-Versuche, die sich eine Ähnlichkeit mit einer bestimmten Person oder einem Unternehmen zunutze machen.

- **30 %** aller Phishing-E-Mails werden geöffnet und **12 %** der Empfänger klicken dann auch auf den enthaltenen Link oder Anhang.
- **97 %** aller Menschen weltweit können eine ausgeklügelte Phishing-E-Mail nicht korrekt erkennen.



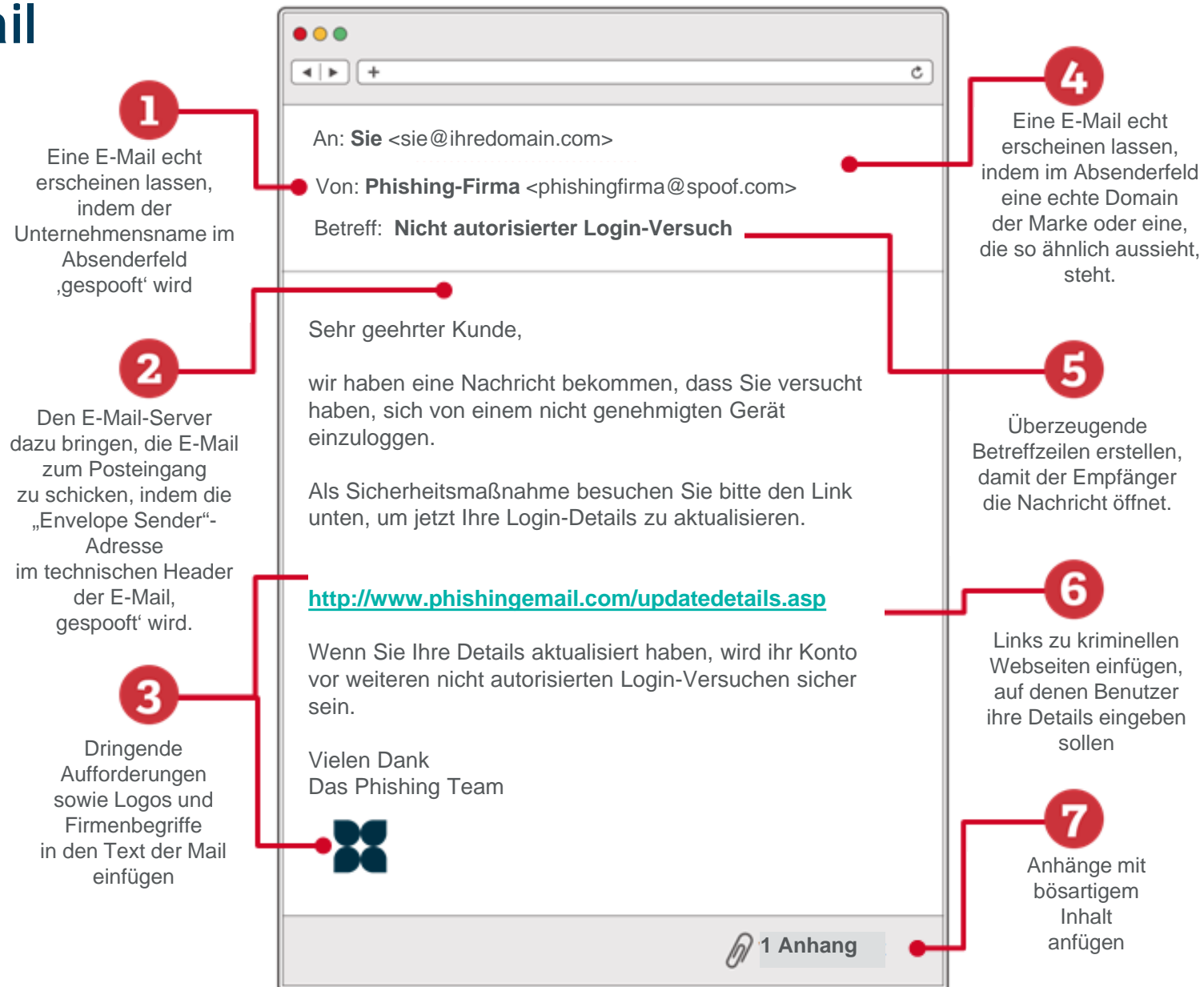
Arten von phishing: Email-Phishing

Außerdem:

- Cyber-Kriminelle entwickeln ihre Taktiken für Phishing-E-Mails immer weiter, um **Spamfilter zu umgehen**.
- Die Verfügbarkeit von Informationen in den sozialen Medien erleichtert die Recherche zum Verfassen einer **überzeugenden** Phishing-E-Mail.
- In einem Zeitalter, in dem jeder jederzeit mit dem Smartphone online ist, **werden E-Mails regelmäßig abgerufen**. Das heißt, dass Phishing-E-Mails früher gelesen werden und sich die **Verwundbarkeit** gegenüber Cyber-Kriminellen erhöht – insbesondere, wenn ein Mitarbeiter denkt, dass er um 9 Uhr abends eine dringende E-Mail von seinem CEO erhält.

Anatomie einer Phishing-Mail

97 % aller Menschen weltweit können eine ausgeklügelte Phishing-E-Mail nicht korrekt erkennen.





Die fünf besten E-Mail-Köder, die bewirken, dass Empfänger klicken

Zitiert von Proofpoint – einem Cyber-Sicherheitsunternehmen der nächsten Generation

„Sehen Sie sich Ihre Rechnung im Anhang an“

„Klicken Sie hier, um Ihr eingescanntes Dokument zu sehen“

„Ihr Paket ist unterwegs“

„Ich möchte eine Bestellung für die angehängte Liste aufgeben“

„Bitte verifizieren Sie diese Transaktion“



E-Mail: Verhaltensregeln

- **Seien Sie vorsichtig mit allen Anhängen, egal von wem sie kommen.** Insbesondere mit Anhängen in verdächtigen Formaten wie .zip, .exe.
- **Fahren Sie mit der Maus über die Links (ohne zu klicken), um sich zu vergewissern, dass sie zu den korrekten Website-URLs führen.** Stellen Sie sicher, dass dies auch wirklich die Webseite ist, die Sie besuchen wollen. Hier können Sie sehen, ob die Zielseite des Links wirklich zu der Marke gehört, die Sie aufrufen wollen, und nicht zu einer Fälschung dieser Marke (in diesem Fall sind einige nicht identifizierbare Wörter, Buchstaben und Zeichen enthalten). Wenn Sie Zweifel haben, klicken Sie nicht darauf.
- **Wenn Sie bei E-Mails auf „Antworten“ klicken, überprüfen Sie immer die E-Mail-Adressen Ihrer Empfänger.** Alternativ können Sie die Adressen eingeben oder von einem Adressbuch einfügen. Der Grund dafür ist der gleiche wie bei der Überprüfung der URL der Webseite.

E-Mail: Verhaltensregeln

- **Verwenden Sie Spamfilter und aktualisierte Schutzfunktionen.** Aktualisierte Lösungen zum Schutz gegen Viren, Phishing und E-Mail-Betrug bieten Ihnen einen grundlegenden Schutz. Gehen Sie sicher, dass dieser Schutz regelmäßig aktualisiert wird.
- **Halten Sie beim Besuch von Webseiten Ausschau nach dem grünen Balken und dem S nach HTTP.** Damit können Sie die SSL-Zertifikate (Secure Socket Layer) der Webseite prüfen – ein Nachweis für eine sichere Anmeldung auf Seiten und Formularen, auf denen Sie möglicherweise persönliche Angaben eintragen.

E-Mail: Verhaltensregeln

- **Wenn Sie den Absender nicht kennen, seien Sie vorsichtig mit Links und Anhängen.** SEIEN SIE VORSICHTIG, selbst wenn Sie den Absender kennen. Überprüfen Sie den Inhalt der E-Mail durch einen Telefonanruf bei der betreffenden Person oder kontaktieren Sie das Unternehmen direkt – insbesondere, wenn Ihnen etwas verdächtig vorkommt.
- **Antworten Sie niemals auf E-Mails, die persönliche Angaben oder Zugangsinformationen verlangen, vor allem dann nicht, wenn die Forderung dringend erscheint.** Selbst wenn die Forderung von Ihrem CEO oder CFO kommt. Selbst wenn Sie jemand sind, mit dem die Chefetage regelmäßig kommuniziert. Es schadet nicht, telefonisch oder persönlich bei der jeweiligen Person nachzufragen.

E-Mail: Verhaltensregeln

- **Klicken Sie nicht auf Popup-Fenster**, die Sie zu einer betrügerischen Webseite oder zu einem Malware-Download weiterleiten können.
- **Seien Sie auch vorsichtig mit Live-Chat-Fenstern**, vor allem, wenn nach persönlichen Anmeldedaten gefragt wird.



Verschiedene Arten von Phishing: Telefon

Mit **Voice-Phishing** oder „Vishing“ können per Telefonanruf persönliche Angaben angefordert werden.

Die Telefonnummer des Anrufers wird möglicherweise falsch angezeigt. Durch komplexe automatische Telefonsysteme kann Leuten glaubhaft gemacht werden, dass der Anruf von ihrer Bank kommt, Kreditkarten oder Banküberweisungen betrifft und es sich um einen Notfall handelt!

Es können auch **Textnachrichten** verschickt werden (SMS-Phishing oder „Smishing“), die dann eine unmittelbare Handlungsaufforderung enthalten, wie einen Link zum Anklicken oder eine Nummer, die man anrufen soll, um persönliche Angaben zu „bestätigen“.

Wenn Sie den Link anklicken oder die Nummer anrufen, kann **Malware** auf Ihrem Telefon installiert werden, die zum Diebstahl von Passwörtern dient.

Telefon: Verhaltensregeln

- **Verifizieren Sie immer die Identität des Anrufers.** Wenn Sie antworten, fragen Sie nach der Rufnummer des Anrufers und seiner Durchwahl oder verlangen Sie eine Information, die der Anrufer über Sie haben sollte.
- **Suchen Sie im Internet nach Berichten über diese Nummer.** Unbekannte Anrufernummern oder Ländervorwahlen können ein Hinweis auf einen Voice-over-IP-Anruf oder eine SMS von einem automatischen System sein.
- **Finden Sie die Kundendienstnummer des Unternehmens heraus.** Statt die während des Anrufs oder in der SMS genannte Nummer anzurufen, vergewissern Sie sich auf Ihrer Kreditkarte, Ihrem Kontoauszug oder als letzten Ausweg online, dass es die richtige Nummer ist.

Telefon: Verhaltensregeln

- **Antworten Sie niemals auf Smishing-Nachrichten.** Und klicken Sie niemals auf Links, vor allem nicht auf verkürzte Links, die das Ziel nicht erkennen lassen.
- **Geben Sie niemals Ihre persönlichen Bankdaten preis.** Bewahren Sie Ihre PIN- und CVV-Nummern an einem sicheren Ort auf; Banken verlangen solche Angaben niemals, weil sie ihnen bereits für Ihr Konto vorliegen.



Phishing-Arten: Soziale Medien

Soziale Medien unterliegen wenigen Sicherheitskontrollen. Das macht es einfach für Cyber-Kriminelle, betrügerische Konten anzulegen und reale Unternehmen mit echt aussehenden Logos, Inhalten, Angeboten usw. zu imitieren. Obendrein ist das auch noch gratis. Kriminelle geben auch manchmal vor, Mitarbeiter des imitierten Unternehmens zu sein. Sie fügen einen Link zu einem echten Konto des Unternehmens ein, um das Vertrauen des Nutzers im sozialen Netzwerk zu gewinnen.

- **Jeder fünfte** Phishing-Versuch erfolgt heute über die sozialen Medien.
- Ein Tweet in den sozialen Medien mit Bitte um Hilfe an *@customerservice* kann leicht abgefangen und von *@customer-service* beantwortet werden.



Soziale Medien: Verhaltensregeln

- Seien Sie vorsichtig bei Kommentaren und Antworten zu Ihren Anfragen in den sozialen Medien. Sie könnten von betrügerischen Konten stammen. Nutzen Sie stattdessen offizielle Kanäle, um sich an ein Unternehmen zu wenden.
- Seien Sie vorsichtig, welche Webseiten und Anwendungen Sie mit Profilen in sozialen Medien verlinken.



Soziale Medien: Verhaltensregeln

- **Fügen Sie nicht einfach unverifizierte Kontakte zu Konten in sozialen Medien hinzu**, selbst wenn Sie angeblich zu Ihrem Unternehmen gehören. Hüten Sie sich außerdem davor, Unbekannte, wie Personalvermittler, hinzuzufügen, bis Sie sich über sie erkundigt haben.
- **Klicken Sie nicht auf Links von nicht vertrauenswürdigen Quellen**. Viele soziale Kanäle verwenden verkürzte Links, die die echte URL verbergen. Bei diesen Links kann es sich um Spam oder Malware handeln.
- **Antworten Sie nicht auf verdächtige E-Mails oder Nachrichten**. Dies gilt auch für verdächtige oder ungewöhnliche E-Mails oder Nachrichten von Freunden. Höchstwahrscheinlich wurde nämlich ihr Konto gehackt. Informieren Sie sie unverzüglich mithilfe von anderen Kommunikationsmethoden.
- **Geben Sie niemals vertrauliche und finanzielle Informationen weiter**. Geben Sie selbst in Unterhaltungen, die privat erscheinen, keine vertraulichen Angaben in sozialen Medien weiter, auch keine Fotos, die Kontoauszüge oder Rechnungen enthalten können.



Vermögenswerte des Unternehmens sichern

Reduzierung inhärenter Risiken





Eine mobile Belegschaft

- Es wird erwartet, dass im Jahr 2020 **fast $\frac{3}{4}$** aller Arbeitskräfte in den USA mobil arbeiten werden.
- Bis 2018 werden voraussichtlich **12,1 Milliarden** mobile Endgeräte genutzt.
- Gartner schätzt, dass bis zum Ende des Jahres 2017 **mehr als die Hälfte** der weltweiten Arbeitgeber ihre Mitarbeiter dazu auffordert, “ihr eigenes Gerät mitzubringen”.
- Zu den beliebtesten Apps, die auf Mitarbeiter-Endgeräte heruntergeladen werden, gehören Apps für **E-Mails, Kalender und Kontakte** (84 %), gefolgt von Dokumenten- und Bearbeitungsapps (45 %) und Intranet-Apps (43 %).

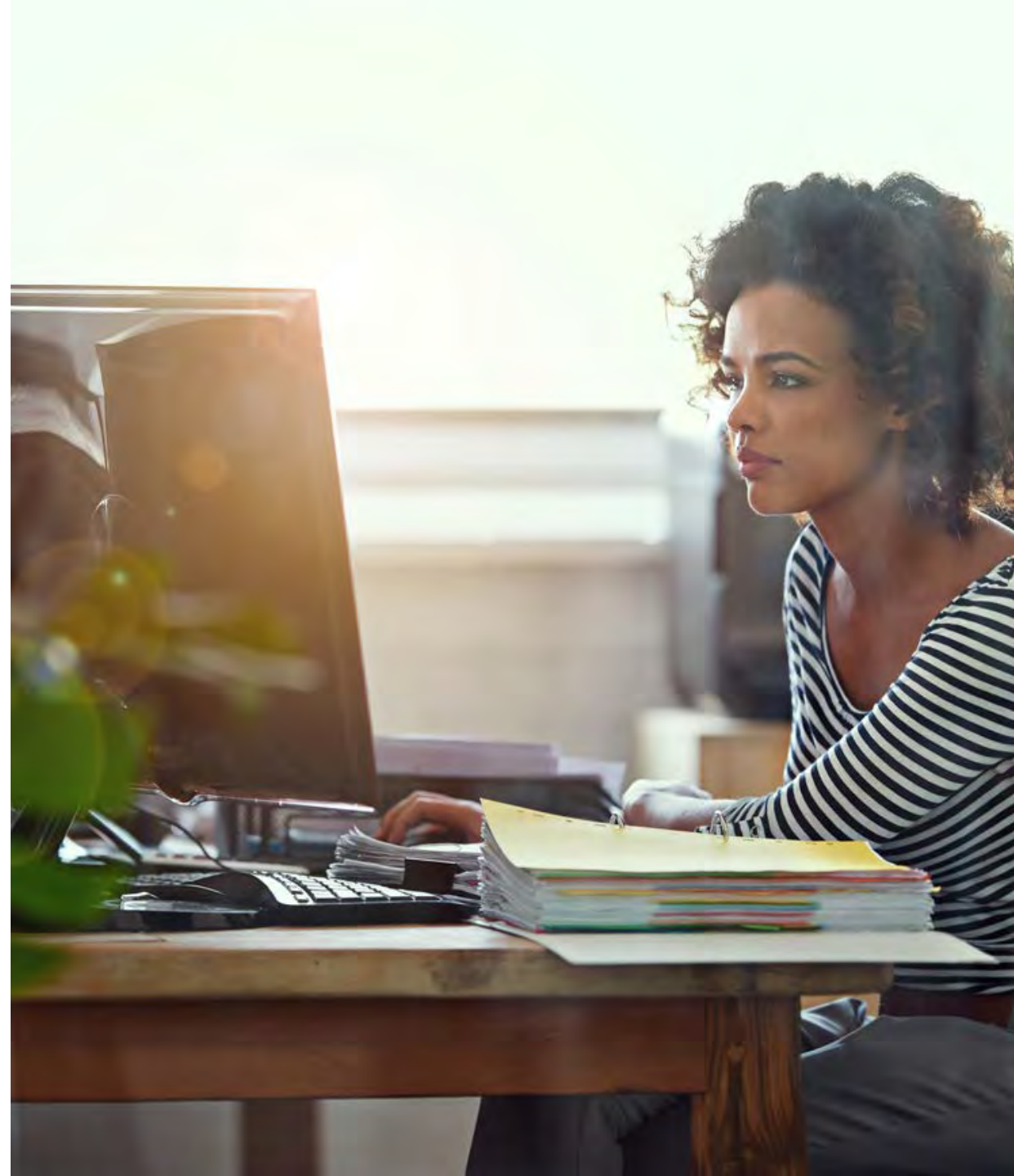




Immanente Sicherheitsrisiken

Ständige Konnektivität bringt immanente Risiken mit sich:

- In einer Umfrage zur Datensicherheit erlitt **1 von 5** Unternehmen eine Sicherheitsverletzung, hauptsächlich weil Mitarbeiter mit ihren Mobilgeräten Malware heruntergeladen oder sich über schädliches WLAN verbunden haben².
- **39 %** der befragten Unternehmen berichteten, dass in der Vergangenheit mit BYOD-Geräten oder unternehmenseigenen Endgeräten Malware heruntergeladen wurde².
- Der durchschnittliche Mitarbeiter trägt zu jeder Zeit **mehr als 2 Geräte** bei sich und fast niemand mehr nutzt Ethernet-Verbindungen, weshalb WLAN ein absolutes Muss ist³.
- Ein hoher Anteil an **WLAN-Hotspots ist unzureichend** oder gar nicht gesichert⁴.



Mobilgerät: Verhaltensregeln

- **Besuchen Sie sichere Webseiten** – achten Sie auf „HTTPS“ in der URL, eine grüne URL und ein Verschlüsselungsschloss – und reduzieren Sie finanzielle Transaktionen in öffentlichen Netzwerken auf ein Minimum.
- **Nutzen Sie ein virtuelles privates Netzwerk**, um Ihre Online-Aktivitäten zu verschlüsseln, insbesondere, wenn Sie eine Verbindung zu einem Unternehmensnetzwerk herstellen.
- Sichern Sie Ihr Endgerät mit **starken Passwörtern**.
- **Aktivieren Sie die Zwei-Faktor-Authentifizierung** für zusätzliche Sicherheit.

Mobilgerät: Verhaltensregeln

- Aktualisieren Sie Software mit Sicherheitspatches, Anti-Viren-Schutz, Spam-Schutz und Spyware-Erkennungsfunktionen.
- Achten Sie auf betrügerisches Phishing und Malware-Links, wenn Sie Ihre E-Mails abrufen.
- Wenn Sie eine Verbindung zwischen Ihrem Bluetooth®-Gerät und Ihrem Handy oder Laptop herstellen, achten Sie darauf, dass Sie sich nicht in einem öffentlichen Bereich befinden, wo Ihr persönlicher Zugangscode (oder PIN) missbraucht werden könnte, und arbeiten Sie mit dem Bluetooth-Gerät stattdessen im verborgenen (nicht sichtbaren) Modus.

Mobilgerät: Verhaltensregeln

- Stellen Sie keine Verbindung zu ungesicherten offenen WLAN-Hotspots her. (Ein Passwortschutz gilt als Anzeichen für eine bestehende Verschlüsselung.)
- Laden Sie keine Programme oder Anwendungen herunter, denen Sie nicht vertrauen.



Passwort- Sicherheit

Die letzte Verteidigungslinie





Die Bedeutung der Passwort-Sicherheit

Ein gutes Passwort ist eine kostenlose und einfache Maßnahme zum Schutz vor Datenschutzverletzungen.

- **80 %** der analysierten Datenschutzverletzungen sind erwiesenermaßen finanziell motiviert.
- **63 %** der Verletzungen waren auf Standardpasswörter sowie schwache oder gestohlene Passwörter zurückzuführen.



Gefährdete Passwörter

Man kann Passwörter als die letzte Verteidigungslinie ansehen, die Cyber-Kriminelle überwinden müssen, bevor sie an Ihre Daten gelangen. Passwörter können gefährdet werden durch:

- **Betrüger, die mit Phishing-Angriffen** persönliche Daten erhalten möchten, wie Benutzernamen, Passwörter, Online-Banking-Daten und vieles mehr.
- **Brute-Force-Angriffe** von Hackern, die systematisch und automatisiert alle möglichen Passwörter und Muster ausprobieren.
- **Eine Datenschutzverletzung** bei einem Unternehmen oder einer gehackten Webseite, die dazu führt, dass Millionen von Konten gefährdet sind.



Gängige Schwächen von Passwörtern

Vor und nach einer Datenschutzverletzung ist ein komplexes Passwort das sicherste. Sie sollten sich an das Passwort erinnern können, aber es sollte eine Besonderheit enthalten, auf die Cyber-Kriminelle nicht kommen können. Verwenden Sie also nicht den Namen Ihres Hundes! Hier sind einige der gängigsten Passwort-Fallen, die Sie vermeiden sollten:

- Die **3 beliebtesten** Passwörter sind *Password1*, *Welcome1* und *P@ssword*.
- Die **gängigsten Begriffe**, die in Passwörtern verwendet werden, enthalten Babynamen, Tiernamen und Städtenamen.
- Fast **30 %** der 10 meistverwendeten Zeichenfolgen haben folgendes Format: Großbuchstabe (U), gefolgt von einer Reihe von Kleinbuchstaben (l) und Zahlen (#), so wie *Ulllll##*, z.B. *Hallo11*.



Passwort: Verhaltensregeln

- Komplexität ist wichtig, aber **die Länge des Passworts ist noch wichtiger**. Die Verwendung von langen Passwörtern (mit mindestens 10 Zeichen) erschwert Cyber-Kriminellen die Entschlüsselung.
- Passwörter mit 8 Zeichen werden unter Anwendung von Brute-Force-Techniken innerhalb von 1 Tag geknackt; bei Passwörtern mit 10 Zeichen werden ca. 591 Tage benötigt. Es dauert also fast 600-mal länger! Verwenden Sie eine Ansammlung von Wörtern, **die Redewendungen** oder Sätze bilden. Sie sollten sie sich merken können, aber sie sollte für andere bedeutungslos sein. Ein Beispiel wäre ***Uzbhazr&fzst*** = Zitat von Walt Disney „Um zu beginnen, höre auf zu reden und fange an zu tun.“ Verwenden Sie immer ein Master-Passwort und einen Passwort-Manager.
- Neben sicheren Passwörtern kann eine **Zwei-Faktor-Authentifizierung** Gefährdungen verringern. Angreifer ziehen lieber zu einem leichteren Zielobjekt weiter, als sich zu bemühen, beide Authentifizierungen zu überwinden.



Passwort: Verhaltensregeln

- **Vermeiden Sie die Verwendung von vorhersagbaren Mustern** wie *Ulllll##* oder nebeneinander liegenden Tasten wie „*qwertz*“ und „*asdf*“.
- **Verwenden Sie in Ihrem Passwort keine Wörter aus dem Wörterbuch** und keine Namen von Familienmitgliedern oder Haustieren, keine Adressen und keine vertraulichen Angaben wie Ausweisnummern, Geburtsdaten, Sozialversicherungsnummern oder Telefonnummern.
- **Verwenden Sie nicht dasselbe Passwort für mehrere Webseiten.** Eine Datenschutzverletzung bei einem Konto würde dann nämlich dazu führen, dass sogar das komplexeste Passwort nutzlos ist, wenn es für mehrere Konten verwendet wird. Verwenden Sie niemals das Passwort Ihres E-Mail-Kontos auf einer anderen Online-Seite.
- **Speichern Sie Ihre Passwörter nicht als normalen Text** auf einem Computer.



Vielen Dank!