Fidelity™ INTERNATIONAL

CYBERSICHERHEIT FÜR JEDERMANN

TIPPS UND HINWEISE FÜR IHRE SICHERHEIT ZU HAUSE, BEI DER ARBEIT, IM INTERNET UND UNTERWEGS

Inhalt

www.fidelity.de

Fidelity™ INTERNATIONAL

Ian Thompson
LEITER DER TECHNIKABTEILUNG *Fidelity International*

Cybersicherheit für jedermann

Cybersicherheit ist ein Kernbestandteil unserer Tätigkeit bei Fidelity.[1]

Mit umsichtigen Maßnahmen zur Cybersicherheit stellen wir sicher, dass nicht nur unsere eigenen Daten, sondern auch die uns anvertrauten Daten unserer Kunden geschützt sind. Diese Broschüre über Cybersicherheit enthält zahlreiche Informationen darüber, dass wir uns der Sicherheitsgefahren beim Thema Datenschutz und Kommunikation stärker bewusst sein müssen. Sie enthält leicht verständliche Hinweise mit einfachen und wirksamen Verfahrensweisen.

Die hier thematisierten Fragen sind gleichermaßen wichtig in unserem privaten Leben wie auch im beruflichen Umfeld. Moderne digitale Kommunikationskanäle machen es möglich, unser Leben mit der Familie, Freunden und Arbeitskollegen praktisch sofort zu teilen. Diese neue Art der Kommunikation hat viele Bereiche unseres persönlichen Lebens bereichert, wirkt sich jedoch auch auf die Erziehung sowie die geistige und soziale Entwicklung von Kindern und Teenagern aus.

Angesichts der damit einhergehenden Vorteile vergisst man manchmal zu schnell, dass die Online-Welt auch Schattenseiten mit sich bringt. Sie dürfen diese Broschüre über Cybersicherheit mit nach Hause nehmen und an Familie und Freunde weitergeben. Hier finden Sie praktische Hilfe und Tipps zu Fragen der Cybersicherheit im häuslichen Umfeld, online und unterwegs.

[1]***www.fidelity.de:*** *Wie Fidelity Sie schützt und wie Sie sich selbst schützen können.*

Fidelity™ INTERNATIONAL

Vorsicht beim Teilen

Soziale Medien können unheimlich viel Spaß machen. Sie ermöglichen es Ihnen, mit alten Freunden in Kontakt zu bleiben (und neue Freunde zu finden), gemeinsame Interessen zu pflegen und auf dem Laufenden zu bleiben. Leider sind Facebook, Twitter, YouTube, Pinterest und LinkedIn auch bei Straftätern sehr beliebt und die Gründe dafür werden Sie überraschen.

Das Internet wird von **3,17 Mrd**. Menschen benutzt, davon sind etwa **2,3 Mrd**. aktiv in sozialen Medien unterwegs. Jeder dieser Benutzer hat durchschnittlich **5,54 soziale Medienkonten**. Die Benutzung sozialer Medien ist allein im letzten Jahr um **176 Millionen gestiegen**.

Quelle: brandwatch.com

Fidelity™ INTERNATIONAL

CYBERSICHERHEIT FÜR JEDERMANN

IN SOZIALEN MEDIEN UNTERWEGS

Wer schon einmal Zeit in sozialen Medien verbracht hat, weiß genau, warum sie so unterhaltsam sind und eine so starke Anziehungskraft haben. Sie äußern Ihre Meinung und erhalten sofort unmittelbare Reaktionen und Feedback. Gelegentlich ergeben sich auch Gesprächsthemen, die das Leben anderer Menschen wirklich verändern können. Soziale Medien beeinflussen alle Aspekte unseres täglichen Lebens – nicht nur bei gesellschaftlichen oder politischen Themen, sondern auch welches Outfit heute passt oder was es zum Abendbrot geben soll.

Jeder weiß jedoch auch von den Schattenseiten sozialer Medien. Wir alle haben schon davon gehört, dass manche Internetnutzer viel zu viele Informationen über sich mitteilen.[2] Vielleicht kennen Sie ja sogar jemanden, der zum Beispiel eine bestimmte Stelle nicht bekommen hat, weil bei einer Internetrecherche nach dessen Namen auf Facebook veröffentlichte peinliche Urlaubsbilder zum Vorschein kamen.

Die reale Gefahr, die jedoch von sozialen Medien ausgeht, sind aktive Straftäter mit kriminellen Vorsätzen, die die gefundenen Daten und Informationen zum eigenen Vorteil ausnutzen. Wir möchten Ihnen nachstehend etwas ausführlicher darlegen, an welchen Daten Hacker besonders interessiert sind und was sie damit machen, wenn sie sie gefunden haben. Auch finden Sie hier allgemeine Tipps und Ratschläge, wie Sie sich sicher im Internet bewegen und nicht mehr als nötig über sich preisgeben.

Hacker beim Datenklau

Stellen Sie sich vor, ich bin ein Hacker und möchte Ihre Online-Identität stehlen. Wenn Sie sich im Internet irgendwo anmelden, z. B. zum Online-Banking oder bei Ihrer Webmail, müssen Sie mehrere Sicherheitsfragen beantworten. Dies sind in

der Regel Fragen nach dem Mädchennamen Ihrer Mutter, dem Namen Ihres Haustiers, Ihrem Geburtsdatum, Ihrem Spitznamen als Kind und so weiter.

Denken Sie jetzt bitte an Ihre sozialen Medienkonten. Angenommen, ich habe Ihre E-Mail-Adresse – wie schwierig wäre es für mich, die Antworten auf die oben genannten Fragen herauszufinden? Gibt es vielleicht süße Bilder von Ihrem Haustier bei Facebook, wo Sie auch dessen Namen erwähnen? Spricht Sie vielleicht jemand in den Kommentaren mit Ihrem Spitznamen an? Wird Ihr Geburtstag erwähnt?

Sie verstehen, was wir meinen.
Sobald ich also meine Recherchen in sozialen Medien beendet habe, muss ich bei Ihrem Webmail-Konto nur auf den Link „Passwort vergessen?" klicken und kann anschließend ganz einfach die persönlichen Angaben, die ich über Sie herausgefunden habe, bei den Sicherheitsfragen eingeben.

[2] ***Mashable.com:*** *10 Personen, die ihre Beschäftigung aufgrund von Fehlern in sozialen Medien verloren haben*

Fidelity™ INTERNATIONAL

Insgesamt haben 60 Prozent der Teenager und jungen Erwachsenen, die im Internet unterwegs sind, schon einmal Fotos von sich in sozialen Medien geteilt, ebenso Bilder von Freunden und Familie.
Die Hälfte aller Teenager und jungen Erwachsenen aktualisieren zudem ihren Status und teilen mit, was sie gerade machen.

Quelle: statista.com

Jetzt habe ich die Kontrolle über Ihr E-Mail-Konto und damit Zugriff auf alle Ihre Online-Konten (da ich ja Ihre gesamten E-Mails sehen kann und somit weiß, wo Sie sich angemeldet haben). Anschließend klicke ich auf „Passwort zurücksetzen". Damit wird eine Aufforderung zum Zurücksetzen an das von mir kontrollierte E-Mail-Konto geschickt, sodass ich jetzt alle Ihre Passwörter ändern kann und Sie aussperre.

Überlegen Sie einmal, welchen Schaden ein Hacker in Ihrem Leben anrichten könnte, wenn er sich einen solchen Zugriff verschaffen würde. Könnte er bei der Bank in Ihrem Namen einen Kredit beantragen? Oder eine neue Kreditkarte bestellen? Bei Amazon nach Herzenslust einkaufen? Oder würde er einfach nur Ihre privaten Geheimnisse ausspionieren...

Achten Sie darauf, was Sie teilen
Erste Regel für einen sicheren Umgang mit sozialen Medien, die trotzdem noch Spaß machen sollen: vor jedem Post nachdenken! Posten Sie keine Informationen, die eventuell zum Hacken Ihrer Online-Konten benutzt werden könnten. Schützen Sie Ihre Privatadresse, E-Mail-Adressen, Telefonnummern und Ihr Geburtsdatum. Ihre Sicherheitsfrage ist ein zusätzlicher Schutz vor Missbrauch – behandeln Sie sie wie ein Passwort. Füllen Sie Ihre Antworten mit komplexen Zahlen- und Zeichenkombinationen oder Ausdrücken aus.

Trennen Sie Ihr privates und öffentliches Leben.
Jeder möchte ab und zu private Dinge mitteilen. Wenn dies unbedingt sein muss, posten Sie diese nur in Ihrem *privaten* Bereich. Überprüfen Sie die Datenschutz- und Sicherheitseinstellungen bei Ihren sozialen Medienkonten, damit nur Freunde und Familie Ihre Seiten sehen können. Die Einstellungen haben einen bestimmten Grund.[3]

Es muss nicht unbedingt die ganze Welt wissen, wo Sie gerade sind.
Wenn Sie jedem erzählen, wo Sie sich gerade aufhalten, sagen Sie natürlich auch, wo Sie gerade nicht sind – nämlich zu Hause. Jeder, der Sie auf Twitter (oder Foursquare, Google Buzz Timeline usw.) beobachtet, weiß genau, wann die beste Gelegenheit ist, bei Ihnen zu Hause einzubrechen.[4]

Schaffen Sie Ordnung
Wenn Sie eine Website nicht mehr benutzen, löschen Sie das Konto. Lassen Sie es nicht einfach aktiv, damit es nicht einfach von jemand anderem übernommen werden kann...

Überlegen Sie zweimal, bevor Sie etwas posten
Alle Online-Posts bleiben für immer im Internet. Nehmen Sie sich immer die Zeit um darüber nachzudenken, was Sie gerade im Internet veröffentlichen wollen. Wären Sie auch nach einem Jahr

„Was in sozialen Medien passiert, bleibt bei Google – für immer und ewig."

YourSocial.com

[3] ***identity.utexas.edu:*** *How to manage your social media privacy settings.*

[4] ***Pleaserobme.com:*** *Sensibilisierung von Menschen, die zu viele Informationen über sich preisgeben.*

Fidelity INTERNATIONAL

(oder selbst am nächsten Morgen) noch sicher, dass andere Ihre Nachricht lesen sollten?

Stellen Sie sich vor, eine andere, von Ihnen geschätzte und respektierte Person, könnte sich beim Lesen Ihrer Nachricht unbehaglich fühlen? Oder könnten Sie sich vorstellen, sich diesen Post für immer auf Ihren Körper tätowieren zu lassen? Wenn die Antwort darauf negativ ist, sollten Sie wahrscheinlich nicht auf „Abschicken" klicken.

Wissen Sie, wer Ihre Freunde sind?
Vielleicht finden Sie es toll, dass Sie eine lange Freundesliste haben, aber wie gut kennen Sie alle diese „Freunde" eigentlich?

Ist es überhaupt möglich, eine solch große, unterschiedliche Gruppe von Menschen zu kennen?

Wenn Sie ihnen so vertrauen, wie Ihrer eigenen Familie, dann können Sie durchaus alles mit ihnen teilen. Aber würden Sie sie z. B. auch bei sich bleiben lassen, wenn Sie nicht zu Hause sind? Ist die Antwort hierauf Nein, sollten Sie lieber zweimal überlegen, bevor Sie sie in Ihr Vertrauen ziehen.

Wenn etwas verdächtig aussieht oder sich verdächtig anfühlt, löschen Sie es
Die Aufforderung zur Anmeldung bei Websites, von denen Sie noch nie gehört haben, Freundschaftsanfragen von Menschen, die Sie nicht kennen, E-Mails und Tweets mit Online-Werbung und unbekannten Links sind wohl bekannte Methoden von Cyberkriminellen, an Ihre persönlichen Daten zu gelangen. Recherchieren Sie, bevor Sie darauf klicken. Oder drücken Sie einfach die Löschtaste zum Entfernen.

Fidelity INTERNATIONAL

Digitale Sicherheit unterwegs

Wenn Sie Ihr Handy, Smartphone, Tablet oder Ihren Laptop regelmäßig benutzen, wenn Sie unterwegs sind, dann sollten Sie Ihre digitale Sicherheit genauso ernst nehmen wie zu Hause. Es ergeben sich nicht nur mehr Gelegenheiten, dass Sie Ihr Gerät verlieren (oder es einfach irgendwo liegen lassen) könnten, sondern Sie nehmen Ihr Gerät aus Ihrem geschützten, privaten WLAN heraus in die große gefährliche Welt.

Es gibt weltweit mehr als **2,6 Milliarden** Benutzer von Smartphones. **87 %** der Menschen haben ihr Smartphone immer bei sich. Im Jahre 2016 gab es **mehr Recherchen** auf Handys als am Computer.

Quelle: deviceatlas.com

Fidelity™ INTERNATIONAL

Heutzutage werden immer mehr vertrauliche Daten auf unseren Mobilgeräten gespeichert – E-Mails, Finanz- und Arbeitsdaten, Unternehmensprofile, Reisepläne usw. Wir wollen auf diese Daten sofort zugreifen können, egal wo wir sind.

Darüber hinaus benutzen wir immer öfter tragbare Hardware, um in der Cloud gespeicherte Daten zu benutzen. Digitale Speicherdienste wie Dropbox, Evernote, Microsoft OneDrive und Apple iCloud ermöglichen es, dass wir von dem Mobilgerät in unserer Hosentasche oder Handtasche aus auf unseren gesamten Datenbestand zugreifen können.

Nicht zu vergessen ist auch der immer stärkere Einsatz unserer Smartphones als Kreditkarten, Smartkeys und Gesundheits- oder Fitness-Tracker (um nur einige zu nennen) und Sie werden verstehen, warum es so wichtig ist, sich vor dem unbefugten Zugriff auf Ihre personenbezogenen Daten zu schützen.

Da Sie Ihr Handy im Prinzip überallhin mitnehmen, wissen Sie selbst, wie hoch die Wahrscheinlichkeit ist, dass es doch einmal verlegt wird, verloren geht, gehackt oder gestohlen wird. Obwohl wir diesen Preis möglicherweise für den ständigen Internetzugang zahlen müssen, können Sie selbst auch Maßnahmen ergreifen, um dieses Risiko zu vermindern.

Nutzen Sie die Voreinstellungen Ihres Geräts
Den einfachsten und wirksamsten Schutz Ihrer Daten können Sie selbst einrichten – nehmen Sie sich die Zeit und beschäftigen Sie sich mit den Sicherheitseinstellungen Ihres Gerätes. Eine Bildschirmsperre, die erst nach Eingabe eines Passcodes aufgehoben wird, ist zunächst einmal der einfachste Schutz gegen zufällige unbefugte Benutzung.[5]

Auffinden und Löschen
Alle Betriebssysteme wie Android, iOS und Windows haben inzwischen standardmäßige Funktionen zum Auffinden/Sperren/Löschen aus der Ferne. Sorgen Sie dafür, dass Sie diese Funktionen aktivieren und sich damit vertraut machen, damit Sie sie im Falle eines Falles, wenn das Gerät nicht auffindbar ist, anwenden können.

Sicherheitsrisiken über WLAN
Wenn Sie kostenloses WLAN in Cafés, Bibliotheken oder anderen öffentlichen Einrichtungen nutzen, sollten Sie sich vor der Anmeldung von einem Mitarbeiter den Netzwerknamen bestätigen lassen. Prüfen Sie auf Ihrem Windowsgerät, ob als Sicherheitstyp WEP oder WPA2 angezeigt wird. Bei Macs und Apple sollte unter den WLAN-Einstellungen ein Schloss-Symbol angezeigt sein.[6] Am Ende der Internetsitzung sollten Sie sich bei allen Netzwerkdiensten auch unbedingt wieder abmelden. Anschließend sollten Sie die WLAN-Daten wieder löschen, d. h. Ihr Gerät sollte das Netzwerk wieder vergessen.

Erstellen Sie ein Backup
Bevor Sie das Haus verlassen, sollten Ihre Daten und Einstellungen auf jeden Fall gesichert werden, denn dann verlieren Sie im Notfall nur das Gerät selbst...[7]

Installieren Sie eine mobile Firewall
Benutzen Sie einen „Reiserouter", mit dem Sie über eine kabelgebundene Netzwerkverbindung in Ihrem Hotelzimmer oder Business Centre einen sicheren mobilen WLAN-Hotspot schaffen, der einen zusätzlichen Schutz vor böswilligen Nutzern bietet, die im gleichen WLAN-Netzwerk sind. Bei vielen Modellen können Sie als zusätzlichen Schutz ein einmaliges Kennwort festlegen.

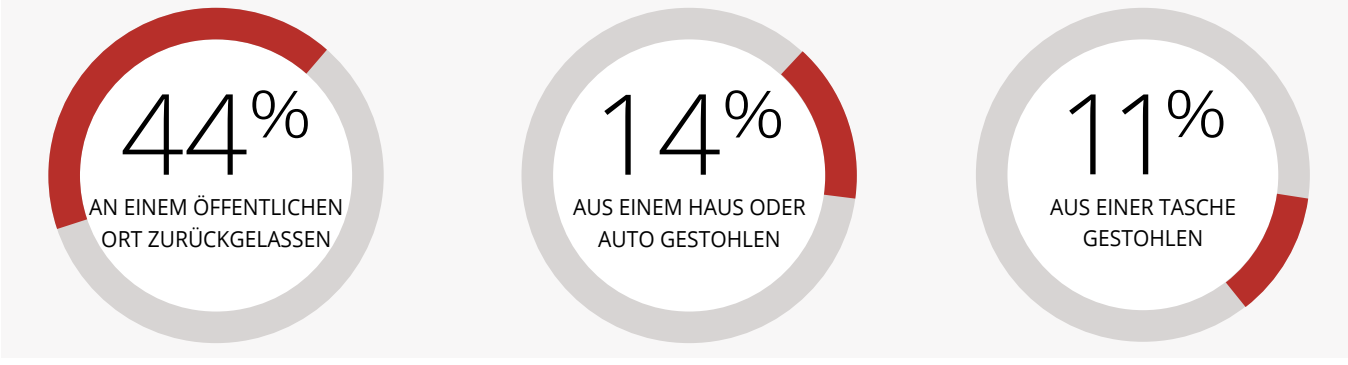
[5] *Lifehacker.com: Wie Sie Ihr gesamtes Betriebssystem verschlüsseln und vor neugierigen Augen verbergen.*

[6] *Lifehacker.com: Die besten Browsererweiterungen, die Ihre Daten schützen.*

[7] *tabtimes.com: Sicherheitsfirma informiert über die Schäden bei Verlust und Diebstahl mobiler Geräte.*

Wie Handys am häufigsten gestohlen werden

Laut einer Umfrage von IDG Research und Lookout Mobile Security war 2014 bei 2.403 Befragten das Handy gestohlen worden.



Alle **53 Sekunden** wird ein Laptop gestohlen. In jedem Jahr gehen **70 Millionen** Smartphones verloren, davon werden lediglich **7 Prozent** wiedergefunden. **80 Prozent** oder Kosten eines verloren gegangenen Laptops sind auf Datenschutzverletzungen zurückzuführen

Quelle:
channelpronetwork.com

Die meisten Laptops haben eine Softwarefirewall installiert, die jedoch durch Viren und andere Schadsoftware deaktiviert werden kann. Benutzen Sie Ihren eigenen WLAN-Router und sorgen Sie so für eine zusätzliche hochwirksame Schutzschicht.

Führen Sie Updates durch

Stellen Sie sicher, dass die Sicherheits- und Systemsoftware aller Geräte jederzeit vollständig mit allen Patches und aktuellen Versionen auf dem neuesten Stand ist. Aktivieren Sie bei Ihren installierten Apps automatische Updates.

Verschließen oder verlieren

Überlegen Sie, ob Sie für Ihren portablen Computer nicht in ein Kabelschloss von guter Qualität investieren sollten. Kabelschlösser sind dünne Stahlseile, die in eine Öffnung an Ihrem Computer passen und an eine fest montierte Installation (z. B. eine Wandhalterung oder Metallstange) angeschlossen werden. Obwohl solch ein Schloss mit etwas Aufwand und genügend Zeit auch durchgeschnitten werden kann, ist Ihr Computer damit für Gelegenheitsdiebe deutlich weniger attraktiv als ein ungesicherter.[8]

Laut Kensington, einem Hersteller von Computerschlössern, werden 40 % der Laptops aus privaten Arbeitszimmern gestohlen. Auf Arbeit zu sein, heißt nicht, dass Sie auch sicher sind.

Am wichtigsten ist jedoch:

Behalten Sie Ihr Gerät immer bei sich und verlieren Sie es nie aus den Augen!

[8] *consumerreports.org: 2013 gab es 3,1 Millionen Diebstähle von Smartphones.*

Fidelity INTERNATIONAL

Mehr Internetsicherheit für Kinder

Kinder lieben Computer und das Internet, das steht außer Frage[9]. Viele Eltern wissen, dass ihre Kinder den ganzen Tag online verbringen würden, wenn sie dürften, weil sie natürlich nur die guten Seiten des Internets sehen. Spiele, Videos, Katzen, Katzenvideos, Chats mit Freunden, Katzen, Antworten auf die verrücktesten Fragen, Klatsch und Tratsch über Prominente, Popmusik, Google Earth und ... Katzen.

Einer aus fünf 8- bis 11-Jährigen und **sieben aus zehn** 12- bis 15-Jährigen haben bereits ein Profil in sozialen Medien. Die Website ChildLine wurde über **3,2 Millionen Mal aufgerufen** – das waren **5 Prozent mehr** als noch 2013/14.

Quelle: nspcc.org.uk

[9] *Internetmatters.org: Hilfe für Eltern und Kinder beim sicheren Umgang mit dem Internet.*

Fidelity INTERNATIONAL

„Kinder, die mit dem Internet aufwachsen, glauben alles, was sie online lesen.“

Ofcom,
Bericht über Medien und die Ansichten von Kindern und Eltern (Children and Parents: Media and Attitudes report)

Wie jedoch bei vielen anderen Dingen im Leben liegen die eigentlichen Gefahren darin, was sie nicht wissen. Sie wissen nichts über Passwortsicherheit, Internet-Trolls und „Netiquette-Regeln“, Phishing, Cybercrime, Hacking und die vielen anderen Sicherheitsfragen, mit denen Erwachsene schon lange vertraut sind.
Das Internet kann ein unkontrollierter und unzivilisierter Ort sein. Niemand will, dass seine Kinder in einem solchen Umfeld unterwegs sind. Trotzdem können sie es kaum erwarten, die unbekannte Online-Welt zu erkunden. Wie geht man also damit um?

Kontrollieren Sie das Umfeld
Alle Anwendungen zum Surfen im Internet haben Sicherheitseinstellungen – machen Sie sich damit vertraut. Es gibt auch leistungsfähige Spezialsoftwareprogramme, mit denen Sie über Filter den Zugriff auf bestimmte Websites und Programme einschränken, Warnungen per E-Mail erhalten, wenn gesperrte Websites besucht wurden und sogar die Tastenanschläge aufzeichnen können.

Bei vielen Kindern ist es wahrscheinlich gar nicht notwendig, sie so stark zu kontrollieren. Sie sollten sich jedoch darüber informieren, welche Möglichkeiten Ihnen zur Verfügung stehen und welche dieser Optionen für Ihre Situation am besten geeignet sind. Gleichzeitig dürfen Sie nicht vergessen, dass kein System hundertprozentig sicher ist.

Bleiben Sie bei Ihrem Kind
Jüngere Kinder sollten unter keinen Umständen allein im Internet surfen. Würden Sie Ihr Kind in eine fremde Stadt mitnehmen und es allein herumlaufen lassen? Würden Sie es den ganzen Tag bei Unbekannten ein- und ausgehen lassen? Lassen Sie Ihr Kind online nicht allein, egal, wie sicher Ihre Sicherheitseinstellungen sind.

Sprechen Sie ganz offen und ehrlich mit Ihrem Kind
Die meisten Eltern wollen, dass ihre Kinder ihre Unschuld bewahren, während sie gleichzeitig eine gewisse Freiheit haben.

Diese Gratwanderung ist nicht immer leicht. Sprechen Sie daher offen und ehrlich mit Ihrem Kind über die Gefahren, die ihm möglicherweise begegnen könnten.

Wie direkt Sie diese Fragen ansprechen wollen, hängt von Ihnen und natürlich von Ihrem Kind ab, aber es ist wichtig, dass Sie die Problematik ungeeigneter Inhalte und die von schlechten Menschen ausgehenden Gefahren zumindest thematisieren.[10] Verängstigen Sie Ihr Kind nicht, sondern bereiten Sie es auf diese Fragen vor, bevor ihm einer seiner Freunde oder das ältere Geschwisterkind etwas Unpassendes erzählt.

Junge „Agenten für Sicherheit"

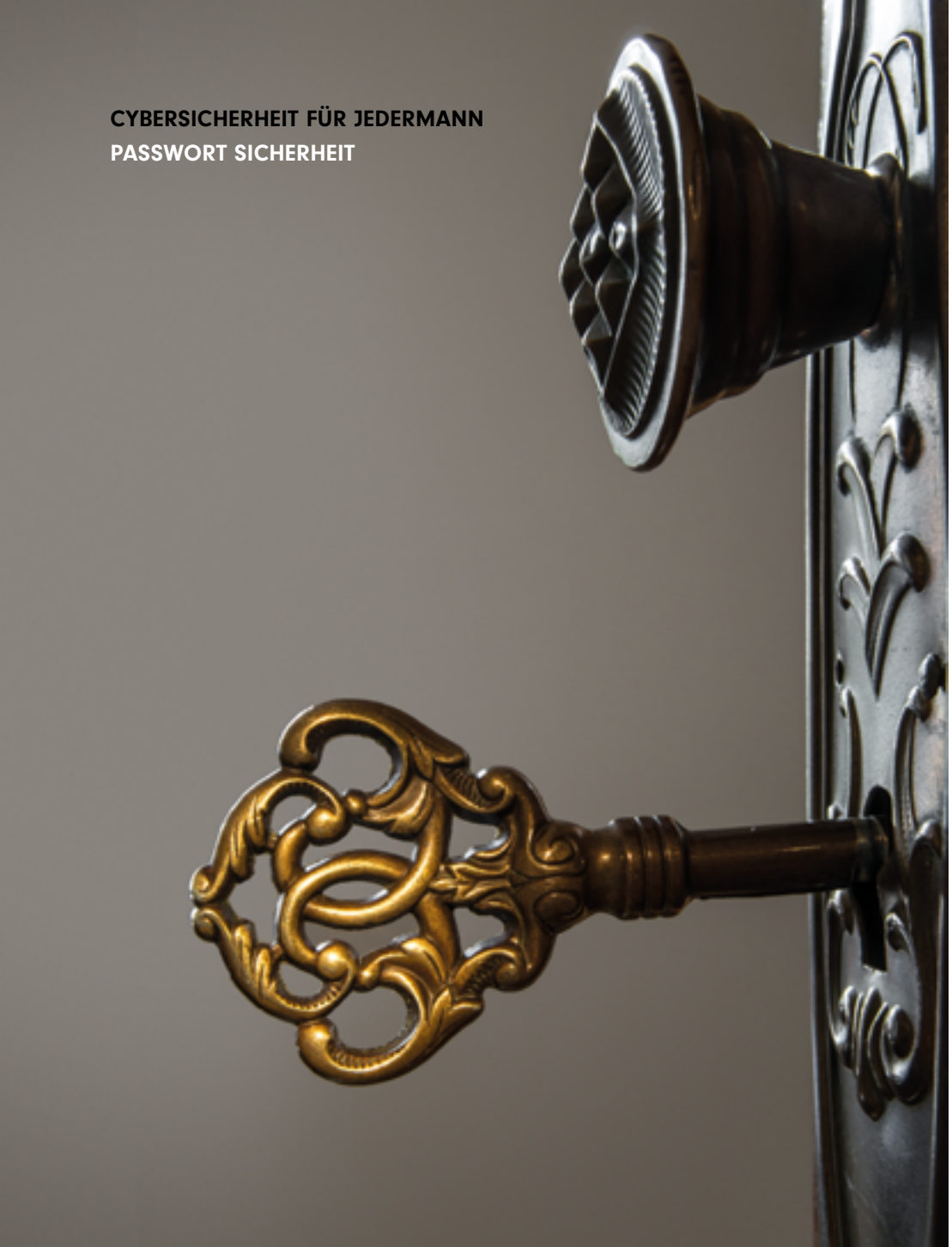
Kinder interessieren sich oft für die Dinge, die ihren Eltern oder älteren Geschwistern Spaß machen. Versuchen Sie daher zu vermitteln, dass kluge Kinder sich auch in der digitalen Welt sicher bewegen können.

Beziehen Sie Ihre Kinder beim nächsten Update der Systemsoftware oder bei der nächsten Installation eines Sicherheitspatches ein. Erklären Sie, warum diese Updates erforderlich sind und wie Ihr Kind dabei helfen kann. Nach erfolgreichem Abschluss können Sie es loben und zum ersten digitalen Sicherheitsagenten der Familie ernennen (vielleicht geben Sie ihm sogar einen Code-Namen?).

Führen Sie gemeinsam mit Ihrem Kind spielerische Sicherheitsrecherchen durch und zeigen Sie ihm, wie es sichere Passwörter erstellt. Lassen Sie Ihr Kind spüren, dass es schon so viel mehr als seine Altersgenossen über Sicherheit im Internet weiß und darauf stolz sein kann. Und bei all dem können Sie vielleicht auch selbst noch etwas Neues lernen!

[10] ***Thinkuknow.co.uk:*** *Testen Sie Ihr Wissen und das Wissen Ihrer Kinder über Internetsicherheit.*

Fidelity™ INTERNATIONAL



Bessere Schlösser und Smartkeys

Passwörter sind die Schlüssel zur digitalen Welt. Wir brauchen sie für den Zugang zu fast allem – vom Bankkonto bis zur E-Mail. Manchmal sind Passwörter umständlich, aber immer unheimlich wichtig zur sicheren Aufbewahrung unserer Informationen. Nachstehend erläutern wir, wie Sie Ihre Konten durch bessere und sicherere Passwörter sichern können.

70 % der Internetnutzer wählen nicht für jede Website ein einmaliges Kennwort. Mit den **10.000 am meisten gemeinsam benutzten Kennwörtern** könnte man auf **98 % aller Konten zugreifen**.

Quelle:
passwordresearch.com

Fidelity™ INTERNATIONAL

2015 kam die US-amerikanische Finanzbehörde IRS in Schwierigkeiten, als sich herausstellte, dass für die meisten ihrer Sicherheitssysteme als Kennwort immer noch „password" benutzt wurde.

Quelle: theguardian.com

Passwörter sind eine Sicherheitsmaßnahme, die einfach zu verstehen und problemlos anzuwenden ist und kaum Kosten verursacht. Passwörter sind inzwischen der Standard für Online-Sicherheit und Identitätsnachweise, und zwar nicht nur gegenüber Unternehmen, mit denen wir täglich Geschäftsbeziehungen pflegen, sondern auch gegenüber Freunden und Familienangehörigen, mit denen wir täglich per E-Mail und in sozialen Medien kommunizieren.

Als es noch einen persönlichen Termin bei der Bank gab hätten wir uns zum Nachweis der Identität noch auf eine Kombination aus Unterschrift, Ausweis, Kontonummer und oftmals der persönlichen Kenntnis des Mitarbeiters am Schalter verlassen. Heutzutage, im Zeitalter des Internets, kennt man uns ausschließlich anhand von zwei Dingen: einem Benutzernamen und einem Kennwort.

Und gerade der Erfolg dieses Verfahrens anhand von zwei Faktoren, Benutzername und Kennwort, führte dazu, dass das System so angreifbar ist. Aufgrund der Tatsache, dass wir für jedes einzelne Konto, Profil, Login und App ein Passwort benötigen, führte das Erfordernis von immer komplexeren Passwörtern zur so genannten „Passwort-Überlastung".

Die Anforderungen an die meisten Benutzer sind einfach unrealistisch[11] und viele Nutzer sehen keinen anderen Ausweg, als gegen die wichtigsten Regeln des Passwortmanagements zu verstoßen: Sie nutzen ihre Passwörter immer und immer wieder für viele verschiedene Websites, sie nehmen so einfache und kurze Passwörter wie nur möglich, die oftmals leicht und schnell zu erraten sind[12] (s. u.).

Wie werden Passwörter gehackt?
Zum Hacken von Passwörtern gibt es mehrere allgemeine Techniken[13]. Viele davon basieren auf einfacher und leicht zugänglicher, bereits erstellter Software, die man ohne weitere Vorkenntnisse anwenden kann. Dazu kommt, dass wir uns durch unsere eigene schlechte „Passwort-Hygiene" oftmals selbst gefährden.

Knacken von Passwörtern:
Stellen Sie sich vor, Sie haben ein Kennwort für ihre Lieblingseinkaufsplattform im Internet, „MeinsicheresPasswort". Wenn

[11] *teamsid.com: Die schlechtesten Passwörter des Jahres 2015.*

[12] *passwordmeter.com*
password.kaspersky.com: Testen Sie die Sicherheit Ihres Kennworts.

[13] *security.blogoverflow.com: Warum Passwörter „zerhackt" werden sollten.*

Die 10 gebräuchlichsten Passwörter des Jahres 2015
Die fünfte jährliche Liste der „schlechtesten Passwörter" von SplashData zeigt, wie sich die Menschen selbst gefährden.

PLATZ	PASSWORT	VORHERIGER PLATZ
1	123456	Unverändert
2	password / Passwort	Unverändert
3	12345678	1 höher
4	qwerty	1 höher
5	12345	2 nach unten
6	123456789	Unverändert
7	football / Fußball	3 höher
8	1234	1 nach unten
9	1234567	2 höher
10	baseball / Baseball	2 nach unten

Sie das Passwort beim Anmelden eingeben, wird es nicht in der Datenbank der Plattform als „MeinsicheresPasswort" gespeichert, sondern „zerhackt".

Hashing („Zerhacken") verwandelt Passwörter, die aus gängigen Wörtern und Zahlen bestehen (Klartext) in beliebige, oftmals bedeutungslose Reihen von Zeichen, genannt *Hash*. Ein Hash für „MeinsicheresPasswort" ist (beispielsweise) Vxc5$MnfsQ4iN$ZMTppKN16y/tIsUYs/ obHlhdP.Os80yXhTurpBMUbA.

Sie merken schon, dass ein Hash überhaupt nicht wie Ihr Passwort aussieht, d. h. wenn jemand das Hash für Ihr Konto herausfinden würde (was heutzutage erstaunlich einfach ist), wären Ihre Daten immer noch sicher. Oder? Falsch! Alles, was ein Hacker benötigt, ist der Hashcode-Zeichensatz und eine kostenlose Software. Damit kann er Ihr Passwort-Hash zurückentwickeln, bis er wieder bei „MeinsicheresPasswort" ankommt. Sie müssen dafür kein Mitglied einer internationalen kriminellen Bande oder Mitarbeiter des Geheimdienstes sein, das schafft fast jedes 12-jährige Kind. Und zwar so:[14]

Wörterbuchangriff: Bei einem Wörterbuchangriff kommt ein Programm zum Einsatz, das eine Datenbank von einer Million Standardwörtern, Ausdrücken, Zahlenreihen, bekannten Redewendungen und Kombinationen durch die Hashing-Software laufen lässt, bis es das richtige Hash für Ihr Passwort findet. Das erfolgt immer und immer wieder, eintausend Mal pro Minute, bis der Begriff „MeinsicheresPasswort" die Zeichenkombination „Vxc5$MnfsQ4iN$ZMTppKN16y/tIsUYs/ obHlhdP. Os80yXhTurpBMUbA" ergibt. Durch die Nutzung einer Wörterbuchdatenbank wird dieser Prozess erheblich beschleunigt, da die meisten Menschen Namen, Orte, Verben, Adjektive und Substantive zum Erstellen von Passwörtern benutzen.

Brute Force: Funktioniert ähnlich wie ein Wörterbuchangriff, jedoch wird nicht versucht, bekannte Wörter und Ausdrücke herauszufinden, die zu dem Passwort-Hash passen, sondern es wird mit „roher Gewalt" versucht, jegliche und sämtliche Buchstaben, Zahlen und Sonderzeichen einzusetzen, um den Kode zu knacken. Stellen Sie sich ein Kombinationsschloss mit einem dreistelligen Zahlencode vor. Eine Brute-Force-Attacke würde versuchen, jede mögliche Zahlenkombination nacheinander auszuprobieren, also zuerst 1-2-3, dann 1-2-4 usw. Dies dauert länger als ein Wörterbuchangriff, ist jedoch sehr effektiv.

Im Januar 2010 untersagte Twitter die Passwörter von 370 Nutzern, weil sie zu offensichtlich waren. Sie enthielten Begriffe wie **„000000"**, **„letmein" (lassmichrein), „aaaaaaaa", „whatever" (egal) und „stupid" (dumm)**.

Quelle: trendhunter.com

[14] *security.stackexchange.com: Was sind die Unterschiede zwischen einem Wörterbuchangriff und der Brute-Force-Methode? fünf Kriterien.*

Ihre Sicherheitsfragen knacken: Viele Menschen benutzen Namen von Familienangehörigen, Haustieren, das Alter, Geburtsdatum, Lieblingsfarbe/-lied/bekannte Sportler und Prominente als Passwortgrundlage. Sollten Sie schon einmal Einzelheiten über irgendwelche dieser Informationen in sozialen Medien erwähnt haben, riskieren Sie, dass Ihre Konten gehackt werden.[15] Vgl. Abschnitt „In sozialen Medien unterwegs" mit Erläuterungen, wie dies gemacht wird und was Sie dagegen tun können.[16]

Die Benutzung einfacher Passwörter: Es wäre unverzeihlich, wenn Sie zu den Internetnutzern gehören würden, welche eins der 10 am häufigsten benutzten Passwörter einsetzen (vgl. S.1 dieser Broschüre). Passwörter, die kürzer als 10 Zeichen sind und keine Kombination aus Großbuchstaben, Sonderzeichen (wie *&^%$£@) oder Zahlen enthalten, bringen Ihre Datensicherheit in Gefahr. Als einer der Hauptgründe, aus denen wir unsere Passwörter nicht in eine deutlich komplexere und schwerer zu knackende Version ändern, wird häufig genannt, dass ja nichts Schlimmes passiert ist ... bisher. Selbst wenn unsere E-Mail gehackt wird, ändern wir häufig nur das Passwort und machen weiter wie zuvor. Warten Sie nicht, bis etwas passiert ist, handeln Sie schon jetzt.

Wiederverwendung von Passwörtern: Es ist schwer, verschiedene Passwörter für E-Mail, Online-Banking, soziale Medien und Einkaufsplattformen zu erstellen und sich zu merken. Wenn Sie aber für alle das gleiche Passwort verwenden, dann sind alle gefährdet, wenn nur eins der Konten gehackt wird. Ein Passwort für alles heißt, Sie könnten alles verlieren.

[15] *slate.com: In welcher Stadt haben Sie Ihre Flitterwochen verbracht? Und weitere überaus dumme Sicherheitsfragen beim Online-Banking.*

[16] *goodsecurityquestions.com: Gute Sicherheitsfragen*

Fidelity INTERNATIONAL

Kennen Sie Ihren Hacker?
Haben Sie schon einmal die Begriffe Black-Hat-Hacker und White-Hat-Hacker gehört und kennen Sie den Unterschied? Der Unterschied besteht in der Hackerethik ...

WHITE-HAT-HACKER
Ein Hacker mit einem „weißen Hut" spezialisiert sich insbesondere auf die Aufdeckung von Sicherheitslücken von Unternehmen und Organisationen.

BLACK-HAT-HACKER
Ein Hacker mit einem „schwarzen Hut" hat umfassende Computerkenntnisse, die er für kriminelle Sicherheitsverstöße einsetzt.

GREY-HAT-HACKER
Ein Hacker mit einem „grauen Hut" hat einen nicht eindeutigen ethischen Kompass und gute Hackerfertigkeiten ohne böswillige Absichten.

HACKTIVIST
Ein Hacker mit politischen oder moralischen Zielen, die häufig mit freier Rede und Menschenrechten im Zusammenhang stehen.

Was können Sie tun?
Alles kann irgendwie gehackt werden, nichts ist unmöglich. Sie können es Hackern allerdings so schwer wie möglich machen, indem Sie die folgenden 10 Punkte befolgen:[17]

1. Benutzen Sie für jedes Ihrer Online-Konten ein anderes Kennwort.
2. Verwenden Sie gegebenenfalls einen Passwort-Manager. Mit einem Passwort-Manager werden Kennwort-Informationen für alle von Ihnen benutzten Websites erstellt, erfasst, verschlüsselt und gespeichert, sodass Sie sich anschließend automatisch anmelden können. Der Zugriff auf den Passwort-Manager erfolgt mit einem Master-Kennwort, das heißt, Sie müssen sich nur ein Passwort merken, alles andere erledigt der Manager für Sie.
3. Überprüfen Sie mithilfe einer angesehenen Website zur Analyse der Passwortstärke, ob Ihr gewähltes Passwort sicher genug ist.
4. Geben Sie Ihre Passwörter nie an öffentlich oder gemeinsam genutzten Computern wie z. B. in Internetcafés oder Bibliotheken ein.
5. Gleiches gilt für ungeschützte, öffentliche WLAN-Verbindungen.[18]
6. Ändern Sie Ihre Passwörter regelmäßig und verwenden Sie ein Passwort nie erneut; ändern Sie es nicht nur minimal ab (d. h. aus SicheresPasswortApril wird SicheresPasswortMai).
7. Geben Sie Ihre Passwörter nicht weiter. Nie.
8. Verwenden Sie mindestens zehn Zeichen und eine Mischung aus Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen. Verteilen Sie die Zahlen unter den anderen Zeichen, setzen Sie Zahlen nicht an den Anfang oder das Ende eines Kennworts. Versuchen Sie beim Erstellen, die maximale Länge eines Passworts auszunutzen, die bei der Website möglich ist, je länger desto besser.
9. Lassen Sie Ihr Gerät nie unbeaufsichtigt und angemeldet.
10. Achten Sie darauf, dass Sie bei der Eingabe Ihres Passworts nicht beobachtet werden.

Es dauert nur **10 Minuten**, um ein aus Kleinbuchstaben bestehendes Kennwort aus **6 Zeichen** zu knacken. Nur zwei Zeichen mehr und ein paar Großbuchstaben verlängern dies auf **3 Jahre**. Und für ein Kennwort mit noch einem Zeichen mehr sowie einigen Zahlen und Zeichen würde man **44.530 Jahre** benötigen.

Quelle:
Stopthehacker.com

[17] ***passwordday.org*** *Hinweise und Informationen zum Erstellen von Passwörtern.*

[18] ***usa.kaspersky.com:*** *Öffentliche WLAN- Netzwerke bergen viele Sicherheitsrisiken, glücklicherweise gibt es jedoch viele Tipps und Hinweise, die man für den sicheren Umgang mit dem Internet anwenden kann.*

Fidelity INTERNATIONAL

Aufmerksamer und sicherheitsbewusster Umgang mit dem Internet

Nicht nur international organisierte kriminelle Banden oder verdeckte Überwachung, sondern auch internationale kriminelle Hacker sind heutzutage allgegenwärtig und darauf vorbereitet, Sicherheitslücken bei neuen und sich entwickelnden Kommunikations- und Datenspeichermöglichkeiten für ihre Zwecke auszunutzen. Die meisten von uns haben keine Probleme bei der Nutzung des Internets, jeder kann jedoch cyberkriminellen Aktivitäten zum Opfer fallen, wenn auf grundlegende Sicherheitsmaßnahmen verzichtet wird.

2014 kam es zu Sicherheitsverletzungen bei den Kreditkarten von **31,8 Millionen** US-amerikanischen Verbrauchern, das war mehr als dreimal so viel wie noch im Jahr 2013. Im ersten Quartal 2015 erhöhte sich der Identitätsdiebstahl im Vereinigten Königreich im Vorjahresvergleich auf **27 Prozent** und macht inzwischen **fast die Hälfte** aller angezeigten Betrugsdelikte aus.

Quelle: nasdaq.com

Fidelity™ INTERNATIONAL

Wissen Sie, was Botnets oder Spywear ist?
Hier ist eine Übersicht über die häufigsten illegalen Aktivitäten zur Infiltration und zum Missbrauch von Computern.

BEGRIFFLICHKEITEN DER CYBERKRIMINALITÄT

Botnets
infizieren Ihren Computer und verwandeln ihn in einen ferngesteuerten „Sklaven" (auch „Zombie" genannt), der von kriminellen Banden für Straftaten in ihrem Namen missbraucht werden kann.

Pharming
Sie werden über eine rechtmäßige URL auf eine gefälschte Fake-Website umgeleitet.

Phishing
Gefälschte E-Mails, SMS und Websites, die anscheinend von echten Unternehmen stammen, aber nur dazu dienen, personenbezogene Daten (wie z. B. Passwörter) von Ihnen zu erfassen oder Sie dazu zu bringen, auf Links zu klicken, um anschließend Ihr System zu infizieren.

Ransomware
Ransomware ist ein Schadprogramm, das sämtliche Daten auf Ihrem Computer verschlüsselt (chiffriert) und eine Mitteilung zur Zahlungsaufforderung anzeigt. Sie werden sozusagen erpresst, eine Zahlung zu leisten, um Ihre Dateien wieder in den Normalzustand versetzen zu lassen.

Spyware
erfasst ohne Ihre Kenntnis Ihre personenbezogenen Daten (Passwörter, Browserverlauf usw.). Sie wird oft ohne Ihre Zustimmung oder ohne Ihr Wissen installiert, wenn Sie eine Datei aus dem Internet herunterladen.

Trojan horse
Schadsoftware, die sich als rechtmäßig ausgibt oder in einem rechtmäßigen (bzw. vorgeblich rechtmäßigen) Programm verbirgt.

Aktivitäten, die auf den ersten Blick vollkommen harmlos scheinen – z. B. die Nutzung von E-Mail-Applikationen, Recherchen im Internet, Herunterladen von Dateien, Spiele und die Anmeldung bei neuen Websites und Diensten, können Ihren Computer oder Ihr Handy durch Viren- oder Spyware-Infektionen gefährden, was zu Datenverlust, Identitätsdiebstahl und sogar schwerem Betrug führen kann.

Wenn Sie dieser Art von Angriffen nicht zum Opfer fallen wollen, können Sie sich am besten verteidigen, indem Sie sich der Tricks und Techniken von Cyberkriminellen bewusst sind und Ihre Daten und Geräte schützen.[19] Denn der Zugriff auf Ihre Daten funktioniert nur, wenn Sie dies zulassen.

Schauen Sie sich im gegenüberliegenden Kästchen einige Begriffe der Cyberkriminalität an – vielleicht sind Ihnen manche bereits bekannt.

Auf den folgenden Seiten werden wir einige davon im Einzelnen besprechen, um zu zeigen, wie sie funktionieren und was Sie zum Schutz dagegen tun können.

Phishing
Phishing ist ein Versuch, meist über E-Mail, auf Ihre persönlichen Daten zuzugreifen oder technische Schäden zu verursachen, um sich finanzielle Vorteile zu verschaffen oder Schaden anzurichten. Phishing-E-Mails enthalten in der Regel einen Link zu einer betrügerischen Website oder einen Anhang mit Schadsoftware. Durch Anklicken des Links oder Herunterladen der Datei wird das Programm aktiviert.

2015 gab es **1.966.324** registrierte Meldungen über versuchte Infektionen mit Schadsoftware, die darauf abzielten, online auf Bankkonten zuzugreifen und Geld zu stehlen.

Quelle: securelist.com

[19] *getsafeonline.org: Zu Ihrem Schutz und dem Ihres Computers.*

Jeden Tag werden Millionen von Phishing-E-Mails weltweit an arglose Opfer versandt. Manche sind einfach als Betrug zu erkennen, andere jedoch sind sehr überzeugend. Können Sie eine echte E-Mail von eine betrügerischen unterscheiden? Hier sind sechs Tipps, wie Sie eine mögliche Phishing-E-Mail erkennen:

1. Die Nachricht hat eine verdächtige oder nicht passende URL
Wenn Sie auch nur den kleinsten Verdacht haben, überprüfen Sie die Integrität der eingebetteten URL-Adressen. Die URL in einer Phishing-Nachricht sieht scheinbar vollkommen richtig aus. Wenn Sie aber mit dem Mauszeiger darüber verweilen, sehen Sie die tatsächliche Adresse, zu welcher der Hyperlink führt. Wenn sich diese Hyperlink-Adresse von der angezeigten Adresse unterscheidet, so handelt es sich wahrscheinlich um einen Betrugsversuch.

2. Die Rechtschreibung und Grammatik der Nachricht ist voller Fehler
Wenn von einem großen Unternehmen eine Mitteilung herausgeschickt wird, werden Rechtschreibung, Grammatik und Rechtmäßigkeit der Nachricht in der Regel überprüft. Enthält eine E-Mail also viele Rechtschreibfehler, so kommt sie wahrscheinlich nicht von der Rechtsabteilung dieses Unternehmens.

3. Sie werden aufgefordert, personenbezogene Daten, insbesondere Passwörter einzugeben
Kein angesehenes Unternehmen wird Sie auffordern, Passwörter oder Anmeldedaten per E-Mail mitzuteilen. Entweder das Unternehmen kennt diese Daten bereits oder es handelt sich um Betrug. Unternehmen haben genügend andere Möglichkeiten, Ihre Identität zu bestätigen.

4. Die Nachricht enthält keine persönliche Anrede oder kundenspezifischen Informationen
Rechtmäßige E-Mails von Banken, Kreditkartenunternehmen

und anderen sicherheitsbewussten Organisationen enthalten oft teilweise dargestellte Kontonummern oder Benutzernamen als Anrede. Eine Begrüßung wie „Sehr geehrter Nutzer" sollte Ihre Alarmglocken zum Läuten bringen.

5. Es ist ein Notfall
Nachrichten, die suggerieren, dass Sie jetzt sofort handeln müssen, um kein Geld zu verlieren oder um zu verhindern, dass Ihnen der Zugriff verweigert wird, haben nur das eine Ziel, Sie ohne Nachdenken zum Handeln zu bewegen. Nehmen Sie sich Zeit und überprüfen Sie den Hyperlink. Versuchen Sie, den Absender auf eine andere Art und Weise zu kontaktieren (Anruf bei einer bekannten Telefonnummer, Besuch vor Ort, manuelle Eingabe der Website-Adresse usw.).

6. Irgendetwas fühlt sich „komisch" an
Vielleicht sieht ein Logo irgendwie ein bisschen anders aus oder die Nachricht ist eigenartig formuliert – manchmal hat man den Eindruck, dass irgendetwas nicht stimmt. Lernen Sie, sich auf Ihr Bauchgefühl zu verlassen. Letztendlich ist die beste Verteidigung gegen Betrug unser gesunder Menschenverstand.

Im Zweifelsfall löschen
Wenn Sie auch nur den geringsten Zweifel an der Rechtmäßigkeit einer E-Mail, eines Links oder Anhangs haben, sollten Sie diese einfach löschen. Öffnen Sie sie nicht, leiten Sie sie nicht weiter, speichern Sie sie nicht, um sie später jemandem zu zeigen. Sicher ist sicher.

Phishing ist also die häufigste Methode von Kriminellen, Ihre persönlichen Daten zu stehlen oder Sie dazu zu bringen, Ihren eigenen Computer zu infizieren. Sobald dies gelungen ist, besteht zum Beispiel die Möglichkeit einer Ransom-Attacke, um Sie zu erpressen:

Digitales Hijacking
Hacker benutzen immer häufiger *Ransomware*,[20] um von Ihnen Geld zu erhalten. Es handelt sich um eine Art digitale Erpressung, die zweierlei Formen hat:

Angriff auf den Anmeldebildschirm
„Lock Screen"-Angreifer sperren einfach den kompletten Zugriff auf das System mit einem Bild, das eine Zahlungsaufforderung und Bankverbindung enthält.

Angriff durch Verschlüsselung
Die Angreifer verschlüsseln sämtliche Dateien auf der Festplatte (oder Netzwerkplatte, auf externen Festplatten, USB-Sticks und sogar Cloud-Speicherbereichen) Ihres Systems und verhindern Ihren Zugriff. Erst nach einer Zahlung erhalten Sie wieder Zugang zu Ihren eigenen Dateien.
Gelegentlich erhält der Nutzer von dem Ransomware-Virus auch eine Nachricht, die angeblich von einer Strafverfolgungsbehörde ist. Darin steht, dass nach Ermittlungen illegale Online-Aktivitäten aufgedeckt wurden und die Festnahme nur durch Zahlung einer Geldstrafe verhindert werden könne.

Was Sie tun können
Es gibt keine Garantie dafür, dass Sie Ihre Dateien zurückerhalten, selbst wenn Sie das Lösegeld zahlen. Sie haben ja auch keine Möglichkeit, sich bei irgendjemandem zu beschweren, wenn sich der Betrüger nicht an die Abmachung hält. Auch ist es heutzutage immer wahrscheinlicher, dass Ihr Erpresser das

[20] *blog.trendmicro.com: Ransomware ist eine der größten Bedrohungen des Jahres 2016..*

Phishing in sozialen Medien

Barracuda Networks befragte Nutzer aus 20 Ländern nach ihren Erfahrungen mit Sicherheitsverstößen und Datenschutzproblemen in sozialen Medien.

54% GABEN AN, SCHON EINMAL EINEN PHISHING-ANGRIFF ERLEBT ZU HABEN	23% HATTEN BEREITS SCHADSOFTWARE ERHALTEN
13% WAR DAS PASSWORT GESTOHLEN WORDEN	17% WAREN OPFER VON DIGITALEM HIJACKING IHRES KONTOS

Ransomware-Virus einfach von einem professionellen kriminellen Hacker gekauft hat und selbst gar nicht weiß, wie er Ihre Daten wiederherstellen sollte, selbst wenn Sie bezahlen würden.

Rechtliche Androhungen sollen Ihnen Angst einjagen und Sie einschüchtern. Diese stammen jedoch nicht von Strafverfolgungsbehörden und sind rechtlich bedeutungslos. Polizeibehörden würden nie auf diese Art und Weise mit Ihnen Kontakt aufnehmen.

Sie sollten sich damit abfinden, dass Ihre Daten unwiederbringlich verloren sind, obwohl es natürlich immer ratsam ist, sich Hilfe von einem Computerfachmann zu holen um herauszufinden, ob Ihr Computer repariert und Ihre Daten wiederhergestellt werden können.

Ein Backup Ihrer wichtigsten und vertraulichen Dateien auf einem externen Speichermedium ist der einzige Weg, mit dem Sie sicherstellen können, dass Ihre Daten sicher sind.

Gehören Sie auch zur Zombie-Armee?

Internetfähige Computer, die mit ferngesteuerten Schadprogrammen namens Bots infiziert sind, bilden ein Botnet/Botnetz.[21]

Botnets sind die lautlosen Jäger der Hackerwelt. Jeder betroffene PC ist ein „Zombie" und wird gesteuert, um gemeinsam mit anderen infizierten Computern in einer Zombie-Armee unter der Kontrolle eines Botmasters zu handeln. So werden Sie möglicherweise als Zombie missbraucht und wissen es gar nicht.

Hat der Hacker einmal sein Botnet installiert, kann er es dafür einsetzen, um eine Website mit Informationsanfragen zu überschwemmen, indem von der Armee der Computer immer wieder die gleiche Anfrage gesendet wird, es zu einer Überladung der Website kommt und diese zusammenbricht (auch Überlastungsangriff genannt). Diese Art von Angriffen kann zur Erpressung von großen Unternehmen und Geldforderungen benutzt werden.

Der Master einer Zombie-Armee kann das infizierte Netzwerk

Ransomware-Programme wurden auf **753.684** Computern von Einzelnutzern entdeckt. **179.209** Computer waren das Ziel von Angriffen durch Verschlüsselung.

Quelle: securelist.com

[21] *welivesecurity.com: Die 5 gefährlichsten Zombie-Botnets.*

Wie Sie erkennen, ob die Sicherheit Ihres Computers gefährdet ist
Computer, die sich infiziert haben, verhalten sich möglicherweise eigenartig – insofern unterscheiden sie sich nicht von uns Menschen. Die folgende Liste soll Ihnen dabei helfen herauszufinden, ob die Sicherheit Ihres PCs gefährdet ist.

CHECKLISTE EINER INFEKTION

Überprüfen Sie anhand der Checkliste, ob die Gesundheit Ihres Geräts oder Systems in Gefahr ist. Überprüfen Sie, ob einer, manche oder vielleicht sogar alle der folgenden Punkte für Sie zutreffen:

- ✔ Unerwartete Pop-ups, die zufällig erscheinen, können auf eine Spyware-Infektion hindeuten
- ✔ Programme starten anscheinend von selbst
- ✔ Ihre Sicherheitssoftware läuft nicht mehr
- ✔ Es dauert deutlich länger, dass Ihr Computer hochfährt, manchmal startet er selbst neu oder lässt sich gar nicht starten
- ✔ Die Darstellung an Ihrem Computer sieht verzerrt aus
- ✔ Es dauert sehr lange, bis ein Programm neu startet
- ✔ Dateien und Daten sind verschwunden oder an einen anderen Ort verschoben
- ✔ Die Systemsoftware bricht ständig zusammen
- ✔ Ihre Homepage hat sich auf mysteriöse Weise verändert
- ✔ Sie haben auf einmal keinen Arbeitsspeicher mehr
- ✔ Dateien und Daten wurden umbenannt
- ✔ Das Surfen im Internet und Laden von Websites ist langsam

Falls Sie der Meinung sind, dass Ihr PC infiziert sein könnte, sollten Sie Ihre Sicherheitssoftware aktualisieren und über den gesamten Rechner laufen lassen. Wenn Sie nichts finden oder sich nicht sicher sind, was Sie tun können, holen Sie sich professionelle Hilfe.

auch dafür missbrauchen, um Millionen von Spam-E-Mails, Viren und Schadprogrammen zu verschicken. Und all dies mithilfe Ihres Computers.[22]

Was Sie tun können
Sie können mehrere Maßnahmen ergreifen, um die Wahrscheinlichkeit zu reduzieren, dass ein Angreifer Ihr System übernimmt:

Firewall
Installieren Sie eine Firewall, mit der Sie den Datenverkehr in und aus Ihrem Computer überwachen und kontrollieren. Richten Sie automatische Benachrichtigungen ein, wenn sich ein Angriff andeutet.

Filtereinstellungen für E-Mails
Intelligente Filterkriterien können die Anzahl und Art der unerwünschten E-Mails reduzieren, die in Ihrem E-Mail-Programm ankommen.

Wachsamkeit ist geboten
Sollten Sie bemerken, dass Ihre Internetverbindung sehr langsam ist, können Sie mit einem Systemtool überprüfen, welche Datenmenge Ihr Modem bearbeitet.

Ist der Datendurchsatz sehr hoch, obwohl Sie nichts herunter- oder hochladen, so könnte dies ein Anzeichen dafür sein, dass Sie Teil eines Botnets sind.[23]

Vertrauen in den technischen Support
Manche Betrüger versuchen sogar, sich als Support-Mitarbeiter Ihres Internetdienstanbieters auszugeben. Sie behaupten, dass Sie den Fernzugriff auf Ihren Computer zulassen müssen, damit

Die 5 schlimmsten Botnet-Länder
Stand: Sept. 2016
1 Indien: 2326660
2 Vietnam: 1009151
3 China: 796087
4 Iran: 651753
5 Pakistan: 458816

Quelle: spamhaus.org

[22] *uk.norton.com/botnet: Bots und Botnets – eine wachsende Bedrohung*

Die drei größten Schädlinge

Viren, Würmer, Pferde? Computerschädlinge mit dem Namen von Lebewesen sollen uns ins Bewusstsein bringen, dass es sich um aktive, gefährliche Eindringlinge handelt, die keineswegs ignoriert werden dürfen...

Computervirus

Ein häufig als E-Mail-Anhang oder zum Herunterladen verschicktes gefährliches Computerprogramm, mit dem Ihr Computer infiziert werden soll. Computerviren werden von Cyberkriminellen oft dafür eingesetzt, um sich Zugang zu Ihrem Computer zu verschaffen, diesen nach personenbezogenen Daten wie Passwörtern zu durchsuchen, die Kontrolle über Ihren Webbrowser zu übernehmen und Ihre Sicherheitsvorkehrungen zu zerstören.

Trojanisches Pferd

Ein Trojanisches Pferd versteckt oder verbirgt sich in legaler Software als ausführbare Datei (exe), die sich selbst installiert und automatisch startet. Nach der Installation kann es Ihre Dateien löschen oder kopieren, Sie über Ihre Webcam beobachten oder alle Ihre Tastenanschläge aufzeichnen.

Wurm

Ein Wurm wird selbst aktiv, ohne sich an Ihre Dateien oder Programme zu hängen. Er versteckt sich im Arbeitsspeicher Ihres Computers und verbreitet sich selbst auf andere Computer des Netzwerks oder über das Internet. Die außergewöhnliche Replikationsrate von Würmern kann nicht nur Einzelpersonen, sondern das Internet selbst in Gefahr bringen.

Mehr als **27 Millionen** Amerikaner fielen in den letzten fünf Jahren dem Diebstahl ihrer Identität zum Opfer. Allein im letzten Jahr wurde die Identität von **9 Millionen** Menschen gestohlen.

Quelle:
stopthehacker.com

angeblich gefährliche Dateien oder Software entfernt werden können, die sich auf Ihrem Gerät befinden würden.
Wenn Sie sich nicht an Ihren Internetdienstanbieter oder das Computer-Helpdesk gewandt haben, können Sie sicher sein, dass es sich bei einem solchen Angebot um Betrug handelt.

Wie die Masche funktioniert

Hacker finden anhand Ihrer Internetprotokoll (IP)-Adresse Ihren Internetdienstanbieter heraus. Sobald sie wissen, wer Ihr Internetanbieter ist, ist es kinderleicht, sich als rechtmäßigen Support-Mitarbeiter von diesem Unternehmen auszugeben.
Dann behauptet der falsche Technikmitarbeiter entweder über ein Chat-Fenster an Ihrem Bildschirm oder telefonisch, dass er die Kontrolle über Ihren Rechner übernehmen muss, um infizierte Dateien aus Ihrem System zu löschen. Nachdem Sie ihm den Zugriff erlaubt haben, werden Sie aufgefordert, eine Zahlung zu leisten, um die angeblich gefährlichen Dateien zu löschen.

Was können Sie tun

Gestatten Sie niemandem den Fernzugriff auf Ihren Computer, den Sie nicht selbst ausdrücklich gebeten haben, an Ihrem Rechner zu arbeiten.[24]

Ignorieren Sie das Chat-Fenster des Helpdesks, schließen Sie es und/oder legen Sie den Hörer einfach auf. Benachrichtigen Sie Ihren Internetdienstanbieter unter der Ihnen bekannten oder bereits benutzten Nummer und erklären Sie die Situation.

Sollten Sie den Fernzugriff gewährt haben, ist Ihr System wahrscheinlich bereits gefährdet. In einem solchen Fall sollten Sie das Gerät ausschalten, Ihr Betriebssystem neu installieren oder einen Computerfachmann bitten, Ihr System wiederherzustellen.

[23] *f-secure.com: Kurze Erklärung von Botnets – was Botnets sind, wie sie funktionieren und welchen Schaden sie anrichten können.*

[24] *moneysavingexpert: 30 Möglichkeiten, Internetbetrug zu unterbinden.*

Cramming ist eine Form von Betrug, bei dem auf der Telefonrechnung zusätzliche Gebühren für Dienste hinzugefügt werden, die der Teilnehmer weder bestellt noch verlangt hatte. Oder es werden Gebühren für Anrufe oder Dienste erhoben, die dem Teilnehmer nicht ordnungsgemäß offengelegt wurden.

Quelle: en.wikipedia.org

Vollständige Backups Ihrer Daten sind dafür unabdingbar.

Betrügerische Anrufe

Betrüger und Cyberkriminelle benutzen jedoch nicht nur die allerneuste Technik des 21. Jahrhunderts, auch das Telefon ist bei Straftätern nach wie vor äußerst beliebt.[25]

Beim „Vishing" oder Voice Phishing rufen Betrüger an und täuschen vor, angeblich im Auftrag Ihrer Bank, des Kabelanbieters oder sogar der Polizei zu handeln. Sie warnen vor angeblich verdächtigen Kontobewegungen und behaupten, Sie wären einem Kreditkartenbetrug zum Opfer gefallen. Das Ziel solcher Anrufe besteht darin, Ihre Kontodaten und Passwörter herauszufinden.

Besondere Vorsicht ist geboten, wenn ...

... Sie jemand anruft und behauptet, Ihre Bankkarte wäre bei einer betrügerischen Transaktion benutzt worden. ... ein Anrufer vorschlägt, dass Sie den Hörer auflegen und zurückrufen sollen, um die Echtheit seiner Identität zu überprüfen. Betrüger können währenddessen jedoch nicht auflegen und in der Leitung bleiben, um vorzutäuschen, dass Sie mit der von Ihnen gewählten Sicherheitsnummer verbunden sind. ... jemand bittet, Geld auf ein neues Konto zu überweisen, selbst wenn behauptet wird, dieses Konto laute auf Ihren Namen.

Was Sie tun können

Lassen Sie sich nie überreden oder unter Druck setzen, etwas zu tun, was Ihnen eigenartig erscheint. Wenn etwas falsch zu sein scheint, überlegen Sie einen Moment ... Scheuen Sie sich nicht, den Hörer aufzulegen. Bleiben Sie höflich, aber nachdrücklich.

[25] *bbc.co.uk: Telefonbetrüger erschwindeln sich 12.000 Pfund von einem Opfer.*

Zusammenarbeit im beruflichen Umfeld

Arbeitgeber hängen heutzutage stärker denn je von ihren Informationssystemen ab, in denen immer größere Datenmengen erfasst, gespeichert und benutzt werden. Sie sind gegenüber ihren Mitarbeitern verantwortlich, offen und ehrlich anzugeben, welche Materialien erfasst und wie diese gespeichert werden. Gleichzeitig sind Mitarbeiter verpflichtet, danach zu fragen. Wie können wir alle dazu beitragen, dass die Sicherheit unserer Daten gewahrt ist?

Laut dem Security Tracker „Shred-it" von Ipsos Reid gaben **47 %** der Befragten an, dass sie für vertrauliche Dokumente sowohl verschließbare Fächer als auch sachgerechte Aktenvernichtungsdienste benutzen, jedoch ist bei **46 %** niemand direkt für die sichere Vernichtung von Daten verantwortlich

Quelle: shredit.com

Fidelity™ INTERNATIONAL

CYBERSICHERHEIT FÜR JEDERMANN

ZUSAMMENARBEIT IM BERUFLICHEN UMFELD

Im Jahr 2015 waren Dritte mit einer Zugangsberechtigung für 41 % der aufgedeckten Sicherheitsvorfälle in Finanzinstitutionen verantwortlich. An 62 % der Sicherheitsverstöße in Industrieunternehmen war ein gegenwärtiger oder ehemaliger Mitarbeiter beteiligt.

Quelle: pwc.com

Wir alle haben das Recht auf einen Arbeitsplatz in einem sicheren Umfeld, sowohl was den Schutz der Gesundheit als auch die digitale Sicherheit angeht. Eine Arbeitskultur mit diesen Ansprüchen lässt sich nicht nur auf die Einhaltung der örtlichen Vorschriften oder Abteilungsrichtlinien zurückführen, sondern ist eine Einstellungssache.

Gleichgewicht der Risiken

Wo Menschen sind, entstehen Risiken, das ist normal. Gleichzeitig sollte jedoch immer auch eine gesunde Ausgewogenheit zwischen Risiko und Freiheit bestehen.

Wenn Sie die Sicherheit Ihrer Daten nicht gewährleisten können, dann ist keine ernsthafte Zusammenarbeit mit Ihrem Unternehmen möglich. Sie müssen dafür sorgen, dass die festgelegten Sicherheitsverfahren Ihre Betriebsabläufe unterstützen, nicht behindern.[26] Informationen und Erkenntnisse müssen fließen können, denn Sie müssen in der Lage sein, auf verschiedene Situationen flexibel zu reagieren ... Alles muss abgewägt werden. Hier sind einige Hinweise, wie wir unsere Daten, unser Kunden und uns selbst schützen können.

Passwörter

Geben Sie Ihre beruflichen Passwörter unter keinen Umständen an Dritte weiter. Das bedeutet auch, dass Sie Ihr Passwort nicht auf einen Klebzettel schreiben und an Ihrem PC-Bildschirm befestigen sollten. Weitere Hinweise finden Sie in dem Abschnitt über Passwörter.

E-Mail

Es ist uns allen schon passiert und es klingt selbstverständlich (es *ist* selbstverständlich), und trotzdem passiert es täglich immer wieder Tausenden von Menschen ... versuchen Sie unbedingt, Ihre E-Mail an die richtige Person zu senden.

Das Verschicken vertraulicher oder sensibler Daten an jemanden, den diese Informationen nichts angehen, ist einer der unangenehmsten und peinlichsten Fehler überhaupt und kann für Ihren Arbeitgeber fatal sein. Überlegen Sie, ob die E-Mail verschlüsselt werden sollte und überprüfen Sie die Adresse des Empfängers, bevor Sie die Nachricht „Abschicken".

Ihre berufliche E-Mail-Adresse sollten Sie ausschließlich für Ihre Arbeit und nichts anderes benutzen. Ansonsten erhöhen Sie nur die Anzahl der eingehenden Spam-Nachrichten und die Wahrscheinlichkeit, dass Sie das Opfer eines Phishing-Angriffs werden (vgl. den Abschnitt zur Cyberkriminalität).

[26] *inspire-success.com: IT-Sicherheit am Arbeitsplatz: unsere zwölf wichtigsten Tipps*

Fidelity INTERNATIONAL

Virtuelle Welt, physische Sicherheit
Der Schutz Ihrer Unternehmensdaten vor kriminellem Zugriff beschränkt sich nicht nur auf vorausschauende Strategien in der virtuellen Welt. Auch im realen Leben können Sie einiges tun.[27]

SICHERHEIT IM REALEN LEBEN

Schweigen Sie nicht, wenn Ihnen etwas auffällt
Wenn es in Ihrer Firma ein Zugangssystem mit Ausweisen gibt oder Identifikationskarten ausgestellt werden, dann haben Sie höchstwahrscheinlich auch eine Sicherheitsabteilung. Sehen Sie jemanden ohne Ausweis oder fällt Ihnen etwas Ungewöhnliches auf, dann sollten Sie dies melden. Sie müssen die Person nicht direkt ansprechen, nur der entsprechenden Stelle Bescheid geben. Kriminelle verlassen sich darauf, dass wir uns nicht trauen, entsprechende Probleme anzusprechen. Beweisen Sie ihnen das Gegenteil!

Sauber und ordentlich
Behandeln Sie sämtliche ihrer Druckmaterialien mit der gleichen Sorgfalt und genauso sicher wie Ihre digitalen Dateien: Vertrauliche Unterlagen sollten nicht auf dem Schreibtisch liegen bleiben, wenn Sie nicht daran arbeiten. Verschließen Sie diese Dokumente am Ende des Tages und vergessen Sie nichts Vertrauliches im Kopierer oder Drucker. Wenn Sie ein ausgedrucktes Dokument nicht mehr benötigen, schmeißen Sie es nicht einfach weg, sondern vernichten Sie es in einem Reißwolf.

Behalten Sie Informationen für sich
Geben Sie Ihre privaten oder vertraulichen Daten niemals an Personen weiter, die Sie nicht kennen, weder telefonisch noch per E-Mail, es sei denn, Sie sind sich bei dieser Person sicher und wissen, warum sie diese Informationen benötigt. Reden Sie in der Öffentlichkeit oder online nicht über vertrauliche Themen, Sie wissen nie, wer mithört...

Sperren Sie Ihren Bildschirm
Immer wenn Sie von Ihrem Computer weggehen, sollten Sie ihn auf Schlafmodus stellen oder eine Bildschirmsperre aktivieren. Wenn sich also jemand Unbefugtes an Ihrem Computer zu schaffen machen will, benötigt er Ihr Kennwort (solange Sie es nicht auf einen Zettel unter Ihrer Tastatur geschrieben haben).

Arbeitsmaterialien zu Hause
Erkundigen Sie sich, ob es die Unternehmensvorschriften zulassen, dass Sie Arbeitsdateien mit nach Hause nehmen dürfen. Falls dies gestattet ist, sollten Sie die Daten verschlüsseln, bevor Sie sie mitnehmen. Daten auf einem USB-Stick sollten mit einem Kennwort geschützt werden, damit die Informationen bei Verlust des Sticks immer noch sicher sind.

Meldung verloren gegangener oder gestohlener Geräte
Wenn Sie ein Gerät verlieren, auf dem arbeitsbezogene Daten enthalten sind, müssen Sie die zuständige Abteilung so schnell wie möglich informieren. Auch wenn es unangenehm ist, den Verlust zuzugeben, es wäre deutlich schlimmer, wenn vertrauliche Informationen in die falschen Hände geraten und Ihr Unternehmen nicht darauf vorbereitet ist.

„Patientendaten sind wie radioaktives Material – sie müssen geschützt und sie müssen eingegrenzt werden. Nehmen Sie sie ernst!“

Arthur R. Derse, MD,
Bioethics Centre, USA

[27] *inspire-success.com: IT-Sicherheit am Arbeitsplatz: unsere zwölf wichtigsten Tipps*

Vor dem Klicken nachdenken
Beim Herunterladen von Materialien aus dem Internet auf Ihren Arbeitscomputer (insbesondere von ausführbaren exe-Dateien) ist Umsicht geboten. Es ist für Sie fast unmöglich zu erkennen, ob sich in einer Datei das verbirgt, was sie vorgibt zu sein oder ob es sich tatsächlich um ein Virus handelt, das nur darauf wartet, die Systeme Ihres Unternehmens zu infizieren.

Kontakt mit Ihrer Sicherheitsabteilung
Wenn es in Ihrem Unternehmen eine Abteilung für IT oder Informationssicherheit gibt, sollten Sie den Kontakt aufnehmen. Erkunden Sie sich danach, wie Ihre Daten gesichert werden und was Sie tun können. Finden Sie heraus, an wen Sie sich wenden können, wenn etwas passiert, damit Sie vorbereitet sind. Vergessen Sie nicht, dass die Mitarbeiter der Sicherheitsabteilung dafür da sind, Sie zu unterstützen. Einer von ihnen hat diese Broschüre geschrieben.

Manchmal werden diese Sicherheitsmitarbeiter vielleicht sogar mit Misstrauen oder als unbequem angesehen, aber bitte denken Sie daran, sie haben mit völlig neuen Gefahren in einem völlig neuen Umfeld zu tun.

Wir sind historisch gesehen die erste Gesellschaft, die mit den Gefahren und Möglichkeiten des Internets umgehen muss. Dies ist für uns alle neu. Manche von uns können mit den damit verbundenen Veränderungen besser umgehen als andere.

Letztendlich leben wir aber inzwischen im digitalen Zeitalter.[28] Früher reichte es aus, abends bei Dienstschluss die Fenster richtig zu verschließen und die Alarmanlage anzuschalten. Heute jedoch sind es nicht nur Bargeld und Geräte, die gestohlen werden können, denn ein Unternehmen, das seine Daten verliert, kann auch seine Kunden und seinen Ruf – also praktisch alles – verlieren. Unser Arbeitsumfeld im 21. Jahrhundert können wir nur gemeinsam schützen.

[28] *cio.com: Wir sind heutzutage alle in der Informationssicherheit tätig*

Fidelity INTERNATIONAL

Kleine Anstrengung, große Wirkung

Das Internet ist nicht der Wilde Westen, es ist nicht der verwunschene Zauberwald, hier verstecken sich nicht unter jeder Brücke Trolle und in jeder Schlucht Banditen. Wir haben Ihnen hier zwar die größten Gefahren des Internets beschrieben, Sie sollten aber nicht denken, dass Sie jetzt nie wieder online gehen wollen. Wir hoffen jedoch, dass wir Sie für Fragen der Internetsicherheit ein wenig mehr sensibilisieren konnten. Bleiben Sie in puncto Sicherheit auf dem neuesten Stand. Wir versprechen Ihnen, das ist keine Zeitverschwendung.

Im 1. Quartal (Jan. bis März) 2015 benutzten **86 % der Erwachsenen (44,7 Millionen)** im Vereinigten Königreich in den letzten drei Monaten das Internet (kürzliche Nutzer), das war 1 % mehr als noch ein Jahr zuvor (Jan. bis März 2014) mit einem Anteil von schätzungsweise 85 %. **11 % der erwachsenen Bevölkerung (5,9 Millionen Menschen)** hatten das Internet noch nie benutzt, was 1 % weniger als noch im 1. Quartal (Jan. bis März) 2014 war

Quelle: ons.gov.uk

Fidelity™ INTERNATIONAL

Mit der Einhaltung einiger vernünftiger Verfahren werden die Chancen erheblich reduziert, dass Sie jemals das Opfer von Cyberkriminalität oder Identitätsdiebstahl werden[29]. Auch Straftäter sind faul und gehen oft den einfachsten Weg, um möglichst viel Gewinn zu machen. So ähnlich wie bei einer Wohnung, bei der die Haustür unverschlossen ist und die Fenster offen stehen, ist hier ein Einbruch wahrscheinlicher, als bei einer verschlossenen Behausung. So kann auch ein Computer oder Konto mit einigen durchdachten Sicherheitsmaßnahmen geschützt werden. Denn ein geschütztes Gerät oder Konto ist für Hacker deutlich weniger attraktiv als eins ohne Schutz. Was wir daraus lernen können, ist klar: machen wir ihnen das Leben nicht ganz so einfach ...

Schützen Sie Ihre Geräte
Regelmäßige Updates Ihres Betriebssystems, Webbrowsers und von Apps ist eine der einfachsten und wirksamsten Maßnahmen zur Sicherheit.

Aktivieren Sie die Einstellung *automatisches Update*, um die neuesten Versionen des Betriebssystems und der Sicherheitspatches zu erhalten.

Schützen Sie Ihre Daten
Benutzen Sie intelligente Passwörter und erstellen Sie für verschiedene Konten unterschiedliche Passwörter. Weitere Informationen finden Sie im Abschnitt *„Passwortsicherheit"* dieser Broschüre.

Verschicken Sie Daten nur über sichere Verbindungen. Achten Sie auf https:// oder das Schloss-Symbol in der Adressleiste, wenn Sie sensible Daten wie z. B. Kreditkartenangaben eingeben.

Melden Sie sich wieder ab, wenn Sie auf einem öffentlichen oder gemeinsam genutzten Computer bei passwortgeschützten Konten oder Websites eingeloggt waren. Schließen Sie am Ende auch das Browserfenster.

Installieren Sie Sicherheitssoftware zum Schutz Ihrer Daten – idealerweise ein Softwarepaket, in dem ein Antivirus-/Malwareprogramm bzw. eine Firewall enthalten sind.

Machen sie nicht zu viel öffentlich
Überlegen Sie, wie Sie soziale Medien benutzen. Prüfen Sie die persönlichen und Sicherheitseinstellungen und bedenken Sie, was ein Krimineller mit den von Ihnen geposteten Informationen anstellen könnte. Schauen Sie sich auch noch einmal den Abschnitt *„In sozialen Medien unterwegs"* an.

Lassen Sie sich nicht verführen
Achten Sie auf Phishing, Links in E-Mails, Tweets, gefälschte Websites und Online-Angebote, die zu gut sind um wahr zu sein – machen Sie es Hackern nicht leicht, auf Ihre privaten Daten zuzugreifen. Seien Sie immer ein wenig misstrauisch und haben Sie keine Angst, etwas zu löschen, was Ihnen komisch vorkommt. Mehr erfahren Sie im Abschnitt *„Cyberkriminalität"*.

Erstellen Sie ein Backup
Es klingt vielleicht ein wenig nervig, aber nur durch regelmäßige Backups aller Ihrer unersetzlichen Fotos, Arbeitsdateien und anderen digitalen Informationen auf einem externen Laufwerk stellen Sie sicher, dass Sie geschützt sind, egal was mit Ihrer Festplatte oder Ihrem Konto in der Cloud auch passiert.

„Lieber Benutzer, liebe Benutzerin des Internets, irgendwann werden Sie einmal wirklich bereuen, dass Sie mich nicht gelesen haben. Mit freundlichen Grüßen, Allgemeine Geschäftsbedingungen …"

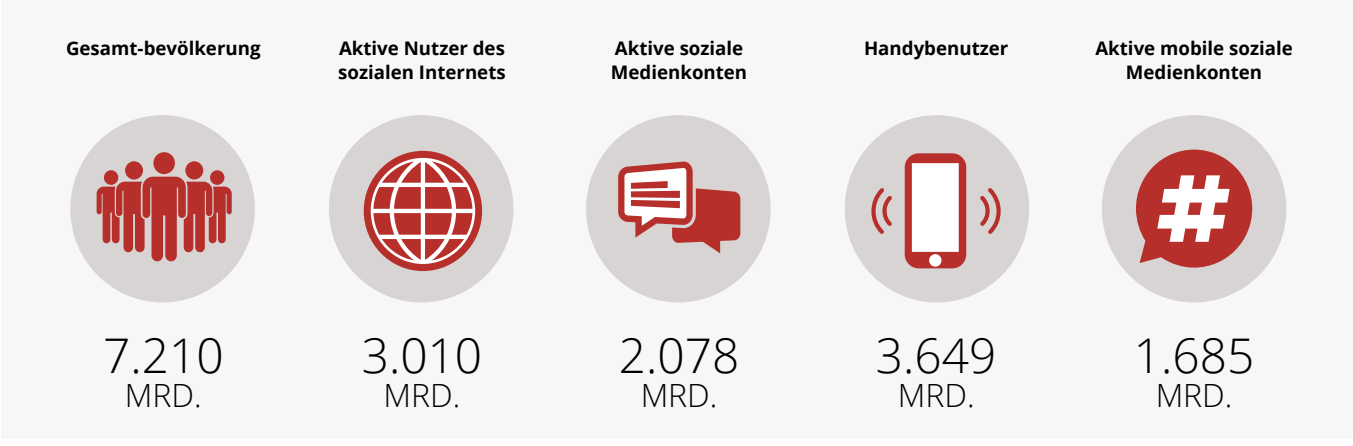
Unbekannter Nutzer,
Facebook.com

[29] *staysafeonline.org: Tipps und Tricks für sicheres Internetverhalten von der nationalen Cybersicherheitsallianz.*

Fidelity INTERNATIONAL

Kurzübersicht der virtuellen Welt

Fast 42 % der Weltbevölkerung hat seit Januar 2015 einen Internetzugang. Wearesocial.net erstellte eine Kurzübersicht über die weltweite digitale Nutzung des Jahres 2015.



Vorbereitung ist alles

Für den Fall der Fälle sollte es einen Plan geben. Verwahren Sie eine ausgedruckte Kopie der E-Mails, Telefonnummern und Adressen Ihrer Freunde und Kontakte auf, falls Ihre Identität gestohlen wird und Ihre Konten gefährdet sind. Vor allem sollten Sie die gültigen Nummern zum Sperren von Kreditkarten und Bankkonten zur Hand haben. Notieren Sie sich die Namen und Telefonnummern der zuständigen Betrugs- oder Strafverfolgungsbehörde, um schnell handeln zu können und den freien Zugang von Straftätern auf Ihre Finanzen einzuschränken.

Denken Sie nach bevor Sie handeln

Viele Betrugsmaschen bauen darauf, dass wir zu begierig sind, das einmalige Superangebot, das nur heute gilt, zum niedrigsten Preis aller Zeiten mitzunehmen. Hinter diesen Betrügereien, die zu gut sind um wahr zu sein, verstecken sich oft gefährliche Absichten. Versuchen Sie, solche Maschen zu durchschauen. Belesen Sie sich, wie andere bereits auf die gleiche Art und Weise betrogen wurden und was der Auslöser war. Natürlich hätten wir alle gern eine kostenlose Urlaubsreise und ein iPad, aber die Chancen, dass dieser Wunsch durch Ausfüllen eines Online-Formulars in Erfüllung geht, stehen gleich Null. Man will Sie über's Ohr hauen.

Und zum Schluss noch eins...

Nur weil die Online-Welt digital ist, bedeutet dies nicht, dass sie nicht echt ist.[30] Sie besteht aus wirklichen Menschen mit einem tatsächlichen Leben und echten Gefühlen.

Es ist manchmal leicht und aufregend, von der Masse mitgerissen zu werden, aber was online passiert, ist von Bedeutung und kann ernsthafte und lang anhaltende Folgen für alle Beteiligten haben. Verhalten Sie sich anderen Menschen gegenüber immer so, wie Sie selbst behandelt werden wollen. Bleiben Sie freundlich, aufmerksam und sicher. Vielen Dank für Ihr Interesse!

[30] *youtube.com: Wie funktioniert das Internet?*

Fidelity INTERNATIONAL

ENDE

Die in dieser Broschüre enthaltenen Daten beruhen auf öffentlichen Quellen, die Fidelity International zugänglich sind. Die Mitarbeiter von Fidelity International haben bei der Zusammenstellung und Verifizierung der Richtigkeit der hier enthaltenen Daten zur Veröffentlichung Sorgfalt walten lassen. Die Inhalte dieser Broschüre könnten jedoch aufgrund von außerhalb der Kontrolle von Fidelity International liegenden Faktoren unrichtig werden und diese Broschüre sollte daher lediglich als Leitfaden benutzt werden.

Mit der Veröffentlichung und dem Vertrieb dieser Broschüre übernimmt Fidelity International weder die Verantwortung für die Ergebnisse von jeglichen Handlungen, die aufgrund von in dieser Broschüre enthaltenen Informationen ergriffen werden, noch für jegliche Fehler oder Unterlassungen, die diese Broschüre enthält. Fidelity International lehnt hiermit ausdrücklich sämtliche und jegliche Haftung und Verantwortung gegenüber jeglichen Personen im Zusammenhang mit Ansprüchen, Verlusten oder Schäden ab, die mittelbar oder unmittelbar aufgrund oder im Zusammenhang mit der Nutzung und dem Vertrauen auf in dieser Broschüre enthaltene Informationen erwachsen. Fidelity International bedeutet FIL Limited bzw. deren Tochtergesellschaften.

Fidelity™ INTERNATIONAL