Identitätsdiebstahl

Bin ich gefährdet? Was kann passieren?
Wie kann ich mich schützen?

WLAN-Router

Muss ich mich auch um die Sicherheit
meines Tors zum Internet kümmern?

Web-Browser

Welche Einstellungen sollte ich ändern,
um meine Sicherheit zu erhöhen?

Alles im **Blick**?

Tipps und Tricks für Ihre
Sicherheit im Internet.

apoBank

Bank der Gesundheit

Inhalt

„Für die Aktualität dieser Tipps und Hinweise übernehmen wir keine Garantie, da sich die digitalen Begebenheiten und Voraussetzungen heutzutage täglich ändern können. Zudem enthalten diese Informationen nicht immer alle Anwendungsfälle für jedes Betriebssystem."

Liebe Leserinnen und Leser,
eine digitale vernetzte Welt bietet den Anwendern viele Vorteile: die Arbeit wird erleichtert, Prozesse verlaufen schneller, Informationen sind jederzeit abrufbar.

Die Kehrseite der Medaille zeigt jedoch, dass durch die permanente und umfangreiche Vernetzung auch Gefahren einhergehen können. So können Daten gestohlen und missbraucht werden, Systeme werden lahmgelegt, Privatpersonen und Unternehmen erpresst. Dabei kann man diesen Risiken durch bestimmte Maßnahmen vorbeugen und diese reduzieren.
Die folgende Broschüre soll Ihnen Aufschluss darüber geben, wie Sie Ihre privaten Geräte optimal nutzen, Ihre Accounts vor fremden Zugriff schützen und dadurch auch Freunden, Verwandten und Kollegen helfen können.

Wir hoffen, Ihnen mit dieser Lektüre konkrete Tipps und Anregungen für eine höhere Sicherheit Ihrer Daten, Informationen und damit Ihrer Identität im Internet geben zu können.

Herzlichst,
Ihr Marcel Breuer
Informationssicherheitsbeauftragter der apoBank

„Private Geräte optimal nutzen, Accounts vor fremden Zugriff schützen und dadurch auch Freunden, Verwandten und Kollegen helfen."

Identitätsdiebstahl – Vom Internet ins wahre Leben.

Identitätsdiebstahl und Identitätsmissbrauch sind zu einem Massenphänomen geworden. Studien zufolge soll schon jeder dritte bis fünfte Deutsche Opfer geworden sein.

Identitätsraub wird häufig für den sogenannten Warenkreditbetrug genutzt, der vergleichsweise einfach umzusetzen ist: Mehr als Ihren Namen und Ihr Geburtsdatum braucht es häufig nicht, um Bestellungen in Ihrem Namen aufzugeben. Online-Handel und Versandhäuser liefern dann die Ware zum Beispiel an eine Paketstation, die der Täter anonym leeren kann.

Die Rechnungen für die Waren gehen an eine andere, falsche Adresse – und deshalb an die Händler zurück.

Über eine Adressermittlung wird das Opfer des Identitätsdiebstahls gefunden. Dieses ahnt derweilen nichts – bis sich Inkassounternehmen bei ihr die Türklinke in die Hand geben und ihr „wegen nicht gegebener Bonität" die Kreditkarte gesperrt wird. Oder sogar ein Haftbefehl gegen sie ausgestellt wird! Für das Opfer stehen Monate der Rechtfertigungen und Richtigstellungen gegenüber seiner Bank, der SCHUFA, gegenüber Gerichten und Inkassounternehmen an.

Laut einer Untersuchung der Beratungsgesellschaft ICF (Inner City Fund) im Auftrag der Europäischen Kommission aus dem Jahr 2022 entstehen Privatpersonen allein aufgrund von Identitätsdiebstählen in Deutschland Schäden i.H.v. 253,7 Millionen Euro.

Alte Tricks in neuem Gewand

Auch der „Enkeltrick" ist in der virtuellen Welt angekommen: Sie erhalten via Internet den Hilferuf eines vermeintlichen Freundes, der – häufig im Ausland – in einer plötzlichen Notlage steckt und dringend Geld benötigt, um nach Hause zu kommen. Dahinter stecken dann Betrüger, die das E-Mail-Konto oder Facebook-Profil Ihres Freundes gehackt oder gefälscht haben.

Täter oder Opfer?

Aber auch umgekehrt kann sich jemand Zugang zu Ihrem E-Mail-Postfach oder Facebook-Profil verschaffen. Dann tritt er in Ihrem Namen auf – mit dem Ziel, Sie gegenüber anderen in Misskredit zu bringen oder zu schädigen. Es kann zum Beispiel sein, dass Täter in Ihrem Namen andere beleidigen oder gar einen Amoklauf ankündigen. Auch Stalker können mit Ihrem Profil andere Menschen bedrängen oder bedrohen.

Mein Briefkasten macht mir Angst.

Nie weiß ich, was ich darin finden werde: Rechnungen, Mahnungen, Drohschreiben von Inkassounternehmen, oder sogar Schlimmeres.

Je länger ich weg bin, desto größer wird meine Angst: Was erwartete mich diesmal, wenn ich nach Hause komme?

„Da Sie auf die vorbenannten Forderungen noch immer nicht reagiert haben, leiten wir jetzt das Mahnverfahren ein", lese ich immer wieder. Ich hätte Waren bestellt – bei mir unbekannten Unternehmen. Lieferungen und Rechnungen wurden an Adressen geschickt – die ich nicht kenne.

Die Diskussionen mit den Inkasso-Unternehmen kenne ich inzwischen. Über Monate hinweg habe ich praktisch täglich solche Post erhalten. Diese ging einher mit Einträgen ins Schuldnerverzeichnis, die ich immer wieder umständlich löschen lassen musste. Diese Fremdbestimmung über mein Leben belastet mich.

Das aller Schlimmste war jedoch, als sogar ein Haftbefehl gegen mich vorlag. Damals suchte die Polizei nach mir in einer falschen Stadt und so wurde ich in Abwesenheit verurteilt! Währenddessen lebte ich mein Leben weiter und ahnte von nichts!

All das, weil meine Daten gezielt für Betrugsdelikte genutzt werden.

Angaben eines Opfers zu den Folgen eines umfassenden Identitätsdiebstahls.

Quellenangabe: op.europa.eu

Namen und die zugehörige Telefonnummer oder gar das Geburtsdatum lassen sich im Internet massenhaft finden. Die Möglichkeiten des Identitätsdiebstahls haben damit deutlich zugenommen. Eine Studie im Auftrag von web.de aus dem Jahr 2022 zeigt auf, dass eine Mehrheit der Befragten befürchten, dass Unbefugte in Ihrem Namen Einkäufe tätigen (72 Prozent) oder Verträge abschließen können (63 Prozent).

Aufgepasst und mitgedacht

Was können Sie tun, um sich gegen Identitätsdiebstahl zu schützen?

Den ersten Schritt machen Sie in diesem Moment: Informieren sie sich über die Gefahren, die in der digitalen Welt zu erwarten sind!

Darüber hinaus finden Sie in dieser Broschüre zu verschiedenen Schwerpunktthemen Tipps und Hinweise, wie Sie sich schützen können, um nicht Opfer von Cyber-Kriminellen zu werden.

Sollten Sie den Verdacht haben, dass Sie Opfer eines Identitätsdiebstahls geworden sind, so können Sie dies der SCHUFA melden. Unter diesem Link steht ein Formular der SCHUFA zur Meldung und weitere Informationen zur Verfügung. Wenn Sie weitere vertiefende Informationen zum Thema Identitätsdiebstahl suchen, empfehlen wir Ihnen insbesondere die Webseite der Verbraucherzentrale mit weiterführenden Links.

Quellenangabe: web.de

Unsere Tipps für Ihren Schutz

- Wenn Sie mehrere Dienste nutzen, können Sie einer Verknüpfung Ihrer Profile zu einem aufschlussreichen Gesamtprofil entgegenwirken, indem Sie **unterschiedliche Nutzernamen** verwenden.
- Verwenden Sie unbedingt **für jeden Dienst ein eigenes Passwort**. Sollte Ihr Facebook-Konto gehackt werden, ist wenigstens Ihr E-Mail-Konto sicher (siehe auch Seite 5).
- Geben Sie bei der Anmeldung bei einem Dienst nur so viel von sich preis, wie jeweils **unbedingt notwendig** ist. Ihr Geburtsdatum zum Beispiel sollten Sie nach Möglichkeit verschweigen.
- Erzählen Sie online nichts über sich, was Sie nicht auch **Fremden** in der U-Bahn erzählen würden. Schon aus der Angabe Ihres Berufes kann auf Ihre Kreditwürdigkeit geschlossen werden.
- Melden Sie sich nicht bei einem Dienst an, wenn Ihnen jemand über die Schulter sehen kann.
- Denken Sie daran, dass Ihr mobiles Gerät **verloren** gehen oder **gestohlen** werden kann, insbesondere wenn Sie jemand bei der Eingabe einer PIN beobachtet hat. Speichern Sie daher auf Ihrem mobilen Gerät keine Passwörter in unverschlüsselter Form oder zur Autovervollständigung!
- Vorsicht vor Phishing-Mails, klicken Sie nicht auf Links zu „lustigen" oder „skandalösen" Videos. Dahinter verbergen sich möglicherweise präparierte Webseiten oder Malware. Dasselbe gilt für Kurz-URLs, die Ihnen Fremde zuschicken. **Allein das Öffnen einer Webseite kann bereits Schadsoftware herunterladen!**
- Halten Sie **alle** Anwendungen (Adobe Reader, etc.) und Softwarekomponenten Ihres Gerätes aktuell, denken Sie dabei auch an nicht häufig genutzte Komponenten.

Das Angeln nach Ihren **Daten**

Phishing: Das klingt nach fischen gehen – und genauso ist es auch. Das Wort setzt sich aus „Password“ und „fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Über gefälschte E-Mails, Webseiten, oder auch mit Kurznachrichten oder Anrufen wird beim Phishing versucht, an die persönlichen Daten eines Nutzers zu gelangen. Im Fokus steht dabei der Erhalt von Benutzernamen und Passwörter, um mit der angeeigneten Identität Straftaten zu begehen.

Sicherheit im Internet

Sie erhalten in der Regel eine E-Mail, die angeblich von Ihrer Bank oder einem Ihnen vertrauten Unternehmen stammt. Darin werden Sie aufgefordert, einem Link zu folgen und dort Ihre persönlichen Daten einzugeben. Bei meist täuschend echt nachgemachten Zielseiten handelt es sich meist um eine Fälschung, die lediglich dem Ausspionieren Ihrer Daten gilt.

Kleine Dinge machen den Unterschied

Sie werden für die Dateienabgabe über einen Link auf eine Internetseite geführt, die zum Beispiel der Bank-Homepage ähnlich sieht. Auf den ersten Blick scheint noch alles normal, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen dazu oft Adressen, die sich nur minimal von echten Internetadressen unterscheiden. Aber manchmal fälschen die Betrüger die Adressleiste des Browsers. Man glaubt so, man sei auf einer vertrauenswürdigen Seite, ist aber nicht. Wer einer solchen Seite seine EC-Geheimnummer, Passwörter oder andere Daten anvertraut, der beschert dem Angler fette Beute und kann sich selbst jede Menge Ärger einhandeln.

Unsere Tipps für Ihren Schutz

- Achten Sie auf den Sender einer E-Mail um vorher schon auszuschließen ob es sich um eine Phishing-Mail handelt.
- Oftmals ist die Sprache der Fake E-Mail sehr direkt und signalisiert Handlungsbedarf.
- Auch können die E-Mails in schlechtem Deutsch verfasst sein, da sie von Computerprogrammen automatisch erzeugt werden.
- Die E-Mails können kyrillische oder falsch aufgelöste bzw. fehlende Umlaute enthalten.
- Bei gefälschten Webseiten erscheinen in der Adresszeile oft Internetseiten, die den echten ähnlich sind, aber unübliche Zusätze haben.

Details zur Erkennung von Phishing E-Mails finden Sie auf der Website BSI für Bürger. Wenn wissen wollen was Sie tun können wenn Sie eine Phishing E-Mail gefunden haben, empfehlen wir Ihnen die Webseite der Verbraucherzentrale.

Schnell geteilt – **lang bereut?**

Über soziale Netzwerke können Sie mit Familie, Freunden, Kollegen und Bekannten kommunizieren, Ihre Fotos und Videos teilen und vieles mehr. Mit einigen wenigen Tipps bleibt Ihnen die Freude daran erhalten, und der Diebstahl Ihrer Identität wird den Cyber-Kriminellen erschwert.

Soziale Netzwerke sind Teil unseres Alltags. Ob Nachrichten, Videos oder Fotos – für jeden Geschmack gibt es eigene Plattformen. Wo so viele Daten preisgegeben werden und so viel Kommunikation stattfindet, ist es wichtig, das Thema Internetsicherheit stets im Auge zu behalten. Datensparsamkeit und der Unterschied zwischen öffentlicher und privater Kommunikation sind wichtig!

Kenne ich dich?

In sozialen Netzwerken tummeln sich oftmals Fake-Accounts, die darauf spekulieren, persönliche Daten von anderen Nutzern abzugreifen. Sofern Sie Freundschaftsanfragen von fremden Personen erhalten, prüfen Sie den Account sorgfältig und lehnen Sie die Anfrage ab! Oftmals verbergen sich hinter neuen Mitgliedern, die sofort viele Kontakte haben, geschickte Betrüger.

Auch von privaten Nachrichten in sozialen Netzwerken kann eine Gefahr ausgehen. Hacker übernehmen Accounts von fremden Nutzern, schicken in ihrem Namen schadhafte Nachrichten herum oder Fragen nach Geld. Sofern Sie eine merkwürdige Nachricht erhalten, reagieren Sie skeptisch und Fragen den Absender über einen anderen Kanal (SMS, Telefon etc.), was es mit der Nachricht auf sich hat. Familie, Freunde und Kollegen könnten gehackt worden sein.

Unsere Tipps für Ihren Schutz

- Fotos, Videos oder andere Inhalte kann man kinderleicht in sozialen Netzwerken teilen. Achten Sie stets darauf, mit wem Sie welche Inhalte teilen wollen, und konfigurieren Sie dies in Ihren Privatsphäre-Einstellungen!
- Viele soziale Netzwerke ermöglichen dem Nutzer Zwei-Faktor-Authentifizierung, die sicherer als ein Passwort ist. (s. Seite 11) Nutzen Sie möglichst diese Variante für einen sicheren Log-In in Ihren Account.
- In vielen sozialen Netzwerken kann anderen Anwendungen Zugriff auf Ihren Account gewährt werden. Checken Sie regelmäßig die Liste der von Ihnen erteilten Berechtigungen und entfernen Sie alle Zugriffsberechtigungen, die Sie für unnötig erachten.

Details zum sicheren Umgang mit Social Media finden Sie auf der Webseite BSI für Bürger. Wir empfehlen insbesondere die übersichtliche PDF-Datei „Soziale Netzwerke“ mit den 10 wichtigsten Tipps für Ihre Sicherheit auf Social Media Plattformen.

Ihr **Schlüsselbund** im Internet

Wir müssen unsere Online-Zugänge schützen wie unsere eigene Wohnungstür. Letztere verschließen wir, um Fremden keinen Zutritt zu gewähren. Gleiches gilt für den Zugang zu unseren Online Accounts. Das bedeutet, wir sichern diesen durch individuelle und starke Passwörter ab.

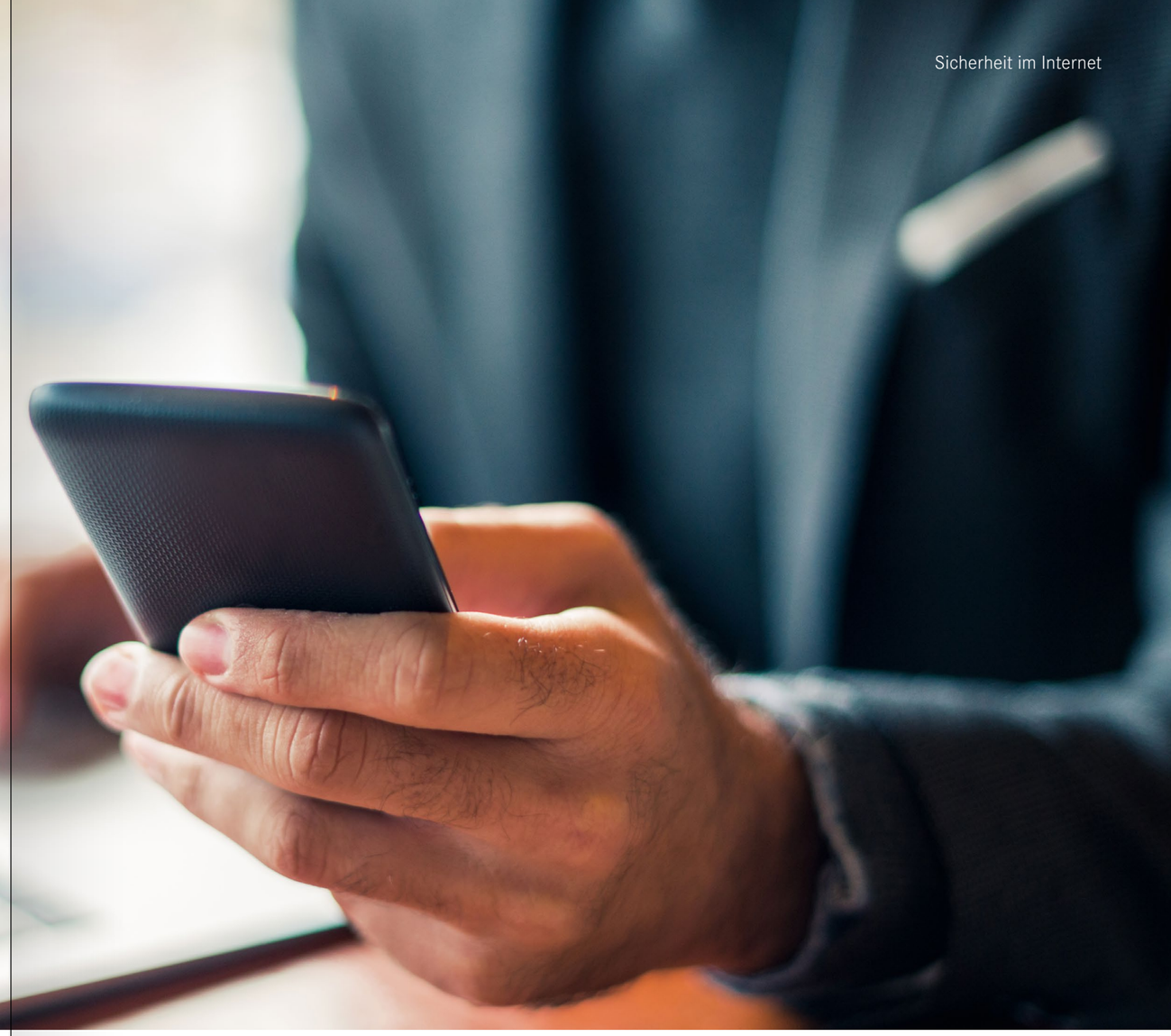
Viele Anwender nutzen aus Bequemlichkeit für verschiedene Webseiten identische Passwörter. Dies ist unbedingt zu vermeiden, da es dem Angreifer erleichtert, durch das Hacken einer Seite auch auf andere Daten zuzugreifen. Wird z. B. bei einer nur wenig geschützten Seite das gleiche Passwort wie für den eigenen E-Mail-Account verwendet, so kann das Bekannt werden eines scheinbar „unbedeutenden" Passworts schnell schwerwiegende Konsequenzen nach sich ziehen.

Nicht irgendein Passwort wählen!

Grundsätzlich gilt: Je länger, desto besser. Passwörter sollten aus mindesten 8 Zeichen, kombiniert aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen, sog. komplexe Komponenten beinhalten. Sollte ein Passwort-Manager verwendet werden, kann dieser automatisch starke Passwörter generieren.

Ungeeignet sind Namen, Geburtsdaten und so weiter. Auch sollte das vollständige Passwort nicht in Wörterbüchern vorkommen und nicht aus gängigen Wiederholungs- oder Tastaturmustern wie „asdfgh" oder „1234abcd" bestehen.

Um sich das Passwort gut merken zu können, gibt es unterschiedliche Strategien. Empfehlenswert ist es, sich einen Satz zu merken, und von jedem Wort den 1. Buchstaben (oder den 2. oder letzten) zu verwenden. Anschließend verwandelt man einige Buchstaben in Zahlen um und fügt Sonderzeichen ein. Ziffern oder Sonderzeichen am Ende des Passwortes anzuhängen oder an den Anfang zu setzen, ist jedoch nicht ratsam.

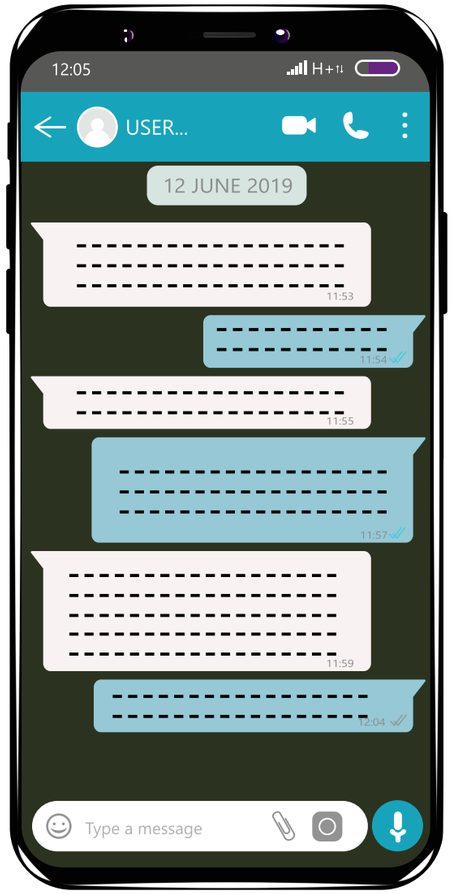


Unsere Tipps für Ihren Schutz

- Nutzen Sie einen Passwortmanager, bspw. 1Password oder KeePass. So müssen Sie sich nur ein gutes Passwort merken und können trotzdem überall sehr starke, unterschiedliche Passwörter verwenden.
- Wichtige Passwörter sollten in regelmäßigen Abständen geändert werden, damit Angreifer im Erfolgsfall nicht dauerhaft Zugriff haben.
- Bei Verschlüsselungsverfahren für WLAN (z. B. WPA, WPA2) sollte das Passwort aus mindestens 20 Zeichen bestehen, da hier auch ohne aktive Netzverbindung Attacken möglich sind.
- Die Zwei-Faktor-Authentifizierung stellt das sicherste Login-Verfahren dar. Hier wird nach dem Einloggen ein weiteres, meist nur einmal gültiges Passwort abgefragt, das über einen gesonderten Kanal übermittelt wird. Dies schützt Ihren Account vor fremden Zugriff, selbst wenn der Hacker bereits Ihre Zugangsdaten kennt.

Alles im **grünen Bereich**

Jeden Monat nutzen 2 Milliarden Menschen aktiv WhatsApp. Da so viele Menschen diesen plattformübergreifenden Messenger verwenden, findet ein immer größerer Anteil der täglichen Kommunikation über diesen Dienst statt.



WhatsApp wurde 2009 gegründet und war schnell die erste Messenger-App, die sich auf den heutigen Smartphones durchgesetzt hat. SMS wurden so durch Kurznachrichten abgelöst, die auch schnell und einfach Fotos, Videos und Grafiken austauschen konnten. In der Anfangsphase noch zahlungspflichtig, ist der Dienst inzwischen kostenlos und plattformübergreifend verfügbar.

Treue Nutzer

Regelmäßig gibt es kleine und große Skandale um WhatsApp, seien es Datenschutzverstöße der Facebook-Tochter oder kritische Sicherheitslücken. Doch die Nutzer kehren dem Messenger nicht den Rücken. Die Nutzung anderer Messenger-Dienste wie Threema oder Signal wäre sicherer, doch diese kamen erst auf den Markt, nachdem WhatsApp sich bereits durchgesetzt hatte. Auf den Punkt gebracht: Es nutzen alle WhatsApp, weil alle WhatsApp nutzen.

WhatsApp für Kinder?

WhatsApp ist in der Europäischen Union erst ab 16 Jahren freigegeben. Als offenes Kommunikationsmedium können Kinder über WhatsApp mit ihnen unbekannten Personen in Kontakt kommen, sowie nicht altersgerechten Inhalten ausgesetzt werden. Zudem forciert WhatsApp unter Umständen Gruppendruck oder Mobbing.

Gemäß einem Urteil des Amtsgerichts Bad Hersfeld haben Eltern bei Minderjährigen für den Umgang mit digitalen Helfern eine Aufsichts- und Aufklärungspflicht. Denn „die Nutzung des Messengers WhatsApp von Kindern und Jugendlichen unter 16 Jahren [kann] grundsätzlich eine Gefahr für deren Privatsphäre und Entwicklung“ darstellen.

Weitere Informationen zu den Einstellungsmöglichkeiten in WhatsApp, aber auch besonders für die Gefahren für Kinder und mögliche Schutzmaßnahmen, finden Sie auf der Webseite Schau hin!, eine Initiative des Bundesministeriums für Familie und anderen.

Unsere Tipps für Ihren Schutz

- Entscheiden Sie bewusst, welche Personen auf welche Informationen Zugriff haben sollen. Die Einstellungen können Sie unter Account ▸ **Datenschutz** bearbeiten.
- Schützen Sie Ihren Account durch eine sechsstellige PIN vor fremden Zugriffen unter Einstellungen ▸ **Verifizierung in zwei Schritten.**
- Achten Sie beim Chatten mit **WhatsApp über den PC** darauf, dass andere Anwendungen nichts mitlesen. Löschen Sie im Menü der App (Knopf mit drei Punkten) unter „WhatsApp Web“ alle Geräte, die Sie nicht nutzen oder kennen.
- Schadhafte **Anhänge** können auch über WhatsApp versendet werden. Öffnen Sie daher keine merkwürdigen Nachrichten von unbekannten Absendern, und begegnen Sie diesen stets mit Misstrauen.
- Damit bei einem Verlust oder Schaden des Mobilgerätes nicht gleich alle Chats und Medien verloren gehen, kann unter Einstellungen ▸ Chats ▸ Chat-**Backup** ein automatisches Backup zu Google Drive oder in die iCloud eingerichtet werden.

Unterwegs im **Internet**

Ein Browser (aus dem englischen Verb „to browse“) ist laut Definition eine Software zur grafischen Darstellung des Internets. Der Web-Browser setzt die Informationen, die Ihnen beim Besuch einer Webseite übermittelt werden, zu der Webseite zusammen, die Sie am Ende vor sich sehen.

Aus diesem Grund stellt der Web-Browser ein zentrales Element auf vielen Geräten dar. Achten Sie darauf, dass stets die neueste Version installiert ist, da der Hersteller durch die Herausgabe neuer Updates bekannte Sicherheitslücken schließt. Darüber hinaus muss sichergestellt sein, dass Ihr Browser automatisch mit Updates versorgt wird.

Durch die Installation von Browser Add-Ons kann zusätzliches Gefahrenpotential geschaffen werden, da diese Zugriff auf alle angezeigten Webseiten haben, auch z. B. Ihrem Online Banking. Diese Add-Ons schauen Ihnen sprichwörtlich über die Schulter! Prüfen Sie vor der Installation unbedingt die Nutzerbewertungen, und idealerweise die Bewertung von Fachzeitschriften. Darüber hinaus sollten Sie immer darauf achten, dass Sie Anwendungen nur von seriösen Anbietern herunterladen.

Kleines s, große (Sicherheits)Wirkung!

Das Hypertext Transfer Protocol, kurz http, wurde durch das Hypertext Transfer Protocol Secure ersetzt (https). Wenn die von Ihnen besuchte Seite https unterstützt, werden durch dieses Verfahren Ihre Daten auf der besuchten Webseite verschlüsselt. Nachvollziehen können Sie das anhand der Adresszeile, in der ein Schloss-Symbol abgebildet ist. Die https-Verschlüsselung ist mittlerweile eine Standradverschlüsselung und viele Browser weisen mittlerweile daraufhin, wenn es sich nur um eine http-Verschlüsselung handelt.

Unsere Tipps für Ihren Schutz

- Browser-Plug-Ins, wie z. B. **Flash und Java,** sind längst überholt und gelten mittlerweile als unsicher. Deinstallieren Sie alle auf Ihrem PC befindlichen Plug-Ins, sofern Sie nicht auf diese angewiesen sind.
- Webseiten können **Berechtigungen** für verschiedene Funktionalitäten anfordern, z. B. zur Standortlokation. Erteilte Berechtigungen können Sie mit einem Klick auf das Schloss-Symbol in der Adressleiste prüfen. Entziehen Sie den Webseiten alle Berechtigungen, die Sie als unnötig erachten.
- Vermeiden Sie es, Webseiten aus zweifelhaften E-Mails zu öffnen. Gefälschte Webseiten werden optisch immer besser! Speichern Sie stattdessen häufig von Ihnen besuchte Webseiten in Ihren **Favoriten** ab, beispielsweise von Ihrer Bank, Ihrer Versicherung, Ihrem Telekommunikationsprovidern sowie die von Ihnen genutzten Einkaufsportalen wie Amazon oder eBay.

Mobile Sicherheit – Hand drauf

Smartphones unterscheiden sich grundsätzlich kaum von modernen Computern und sind ähnlichen Risiken ausgesetzt. Deshalb sind auch hier aktuelle Systeme und der argwöhnische Umgang mit E-Mails und Apps empfehlenswert.

Apple Mobilegeräte

Mobilgeräte von Apple laufen unter dem geschlossenen Betriebssystem iOS. Hardware und Software sind bei diesen Mobilgeräten vom gleichen Hersteller.

- Achten Sie stets darauf, dass Ihr Mobiltelefon durch die Face bzw. Touch ID **gesichert** ist. Alternativ verschlüsseln können Sie Ihr Gerät durch einen Passcode (PIN oder ein Passwort). Für den privaten Gebrauch ist ein Passwort oder einen PIN mit mindestens 6 Zeichen zu empfehlen.
- Prüfen Sie regelmäßig Ihr Endgerät auf die Aktualität der **Updates.** Stellen Sie unter Einstellungen ▸ Allgemein ▸ Softwareupdate sicher, dass Ihr Gerät auf dem neuesten Stand ist.
- Es gibt **Apps,** die auf diverse sensible Informationen Ihres Geräts zugreifen können. Über-prüfen Sie unter Einstellungen ▸ Datenschutz, welchen Apps welche Rechte eingeräumt wurden. Entziehen Sie unnötig erteilte Zugriffsrechte umgehend, und löschen Sie überflüssige Apps.
- Die **Zwei-Faktor-Authentifizierung** zählt für viele Unternehmen zum gängigen Industriestandart, um sich besser gegen Datenverluste und besonders vor Zugriff durch Kriminelle zu schützen. Mit einem Klick in Ihrem Apple Account (appleid.apple.com) auf den Reiter „Sicherheit“ können Sie die Zwei-Faktor-Authentifizierung auch für Ihren Apple-Account einrichten.

Android

Android ist ein freies Betriebssystem, das von verschiedenen Herstellern (z. B. Samsung, Huawei, Sony) auf Mobilgeräten wie Smartphones oder Tablets eingesetzt wird.

- Richten Sie in jedem Fall eine **Display-Sperre** für Ihr Mobiltelefon ein, um bei einem Geräteverlust vor Datendiebstählen geschützt zu sein. Für den privaten Gebrauch ist ein Passwort oder eine PIN mit mindestens 6 Zeichen zu empfehlen.
- Grundsätzlich geben die meisten Hersteller kostenlose **Updates** für modellspezifische Android-Smartphones heraus. Sollte dies nicht (mehr) der Fall sein, sollten Sie sich für die Anschaffung eines neuen Geräts entscheiden, oder zumindest keine kritischen Aktivitäten wie Online-Banking durchführen (per App und im Browser).
- Android Geräte haben den **Virenschutz** „Play Protect“ vorinstalliert. Achten Sie darauf, dass dieser stets aktiv ist (Knopf oben links im Menü des Play Stores). Weitere Virenschutzprogramme werden nicht benötigt.
- Vermeiden Sie die **Installation** von Apps (APK-Dateien) außerhalb des Google Play Stores, da diese deutlich häufiger verseucht sind. Apps aus dem Google Play Store werden von Google überprüft.
- Entziehen Sie Apps **unnötige Rechte** unter Einstellungen ▸ Apps & Benachrichtigungen ▸ App-Berechtigungen, und löschen Sie **verdächtige Apps** umgehend.

Sicher unterwegs

Die meisten mobilen, internetfähigen Geräte können Sie in WLAN-Netzwerke einbinden. Diese Möglichkeit wird von Anwendern oft und gerne genutzt, da die Datenmengen, die sich über das Mobilfunknetz versenden lassen, häufig vertraglich begrenzt sind. Außerdem sind die Übertragungsgeschwindigkeiten über WLAN derzeit meist noch höher als über ein Mobilfunknetz.

Doch die Nutzung eines WLAN-Netzes birgt auch Risiken, vor allem dann, wenn es sich um ein fremdes WLAN-Netz handelt, dessen Betreiber und Hintergründe Sie nicht kennen. Daten können abgegriffen, Schadsoftware auf Ihr Gerät eingeschleust werden.

Daten werden vor der Funkschnittstelle, also vor dem Router, zumeist nicht verschlüsselt und sind für andere Geräte im selben WLAN auslesbar. Ein Angreifer kann dann leicht die Zugangsdaten von Geräten abgreifen, die in das WLAN eingeloggt sind, und den gesamte Datenverkehr mitlesen. Auch verschlüsselte Verbindungen können vorgetäuscht werden!

Virtual Private Network (VPN): Der sichere Tunnel
Rufen Sie vertrauliche Daten über ein fremdes WLAN-Netz am besten nicht ab. Falls das unvermeidbar ist, nehmen Sie dies möglichst nur über eine SSL gesicherte Verbindung (z. B.: https) oder ein VPN (Virtual Private Network) vor. Ein VPN bietet Ihnen eine verschlüsselte Verbindung für sämtliche übertragenen Daten in ein vertrauenswürdiges Netzwerk, sodass unberechtigte Dritte Ihre Daten nicht mitlesen können. Auch die apoBank nutzt ein VPN für die sichere Verbindung zu den Mitarbeitern. Für eine private Nutzung gibt es verschiedene Angebote von Internet-Providern und spezialisierte Dienstleister. Für einen Einstieg in diese Thematik empfehlen wir den Artikel von heise.de, den Sie auf dieser Seite nachlesen können.

Unsere Tipps für Ihren Schutz

- Schalten Sie die WLAN- und Bluetooth-**Funktionen** nur ein, wenn Sie diese benötigen! Ein abgeschaltetes WLAN bietet keine Angriffsfläche.
- Informieren Sie sich über das **Sicherheitsniveau** des Hotspots! In den meisten Hotspots wird nicht verschlüsselt. Lesen Sie die Beschreibungen des Hotspot-Leistungsangebots oder fragen Sie – etwa in einem Café – einfach den Besitzer.
- Deaktivieren Sie nach Möglichkeit die **automatische Anmeldung** an bekannten Hotspots, denn der Name eines WLANs ist frei wählbar. Daher können Betrüger WLANs errichten, die z. B. „Telekom“ oder „Free Wifi“ heißen.
- Deaktivieren Sie die **Datei- und Verzeichnisfreigaben,** damit Ihr Gerät nicht im Netzwerk für andere sichtbar ist.

Weitere Informationen über die Gefahren öffentlicher WLAN Zugangspunkte sowie Details zu möglichen Schutzmaßnahmen finden Sie hier.

Das **Herzstück** nicht vergessen

Ein Betriebssystem, auch OS (von englisch operating system) genannt, ist eine Zusammenstellung von Computerprogrammen, die die Systemressourcen eines Computers wie Arbeitsspeicher, Festplatten, Ein- und Ausgabegeräte verwaltet und diese Anwendungsprogrammen zur Verfügung stellt. Es ist sozusagen das Herzstück eines Computers, zwischen Hardware und Software.

Software auf Ihrem Computer sollte immer auf dem neuesten Stand sein, um externe Gefahren erfolgreich abwehren zu können. Dies gilt für das Betriebssystem genauso wie für einzelne Anwendungen.

Windows 10 Boardmittel

Um sicher zu gehen, dass auf Ihrem PC alle verfügbaren Updates installiert sind, tippen Sie „Updates“ im Startmenü ein und klicken auf „Nach Updates suchen“.

Windows 10 bringt von Anfang an verschiedene Bausteine eines Basisschutzes mit. Diese vorinstallierten Programme müssen aktiviert und gegebenenfalls durch weitere Programme, wie andere Virenscanner, ergänzt werden.

Darüber hinaus empfiehlt es sich, die Festplatte Ihres Notebooks mit BitLocker (Pro-Edition von Windows) oder VeraCrypt zu verschlüsseln. Sollte Ihr Notebook abhandenkommen, ist es vor unbefugten Dritten ausreichend geschützt.

Apple macOS

Auch Benutzer eines Apple-Computers sind Ziel von Kriminellen. MacOS hat ebenfalls unterschiedliche Sicherheitsmaßnahmen integriert. Dass es für Apple-Computer keine Viren geben soll, ist ein Mythos und entspricht nicht der Realität.

Unsere Tipps für Ihren Schutz

- Der vorinstallierte **Windows Defender** ist ein geeignetes Virenschutzprogramm, das zum Schutz Ihres PCs nach aktuellem Stand ausreichend ist. Stellen Sie sicher, dass dieser aktiviert und stets auf dem neuesten Stand ist. Den aktuelle Status des Windows Defenders erfahren Sie, indem Sie im Startmenü „Defender“ eintippen und das Windows Defender Security Center öffnen.
- Um Ihre Daten ausreichend zu schützen, ist es essentiell, regelmäßige **Backups** von Ihrem PC durchzuführen, bevorzugt auf einer externen, abgekoppelten Festplatte.
- Achten Sie darauf, dass die Windows-**Firewall** stets aktiviert ist. Dies können Sie erreichen, indem das Netzwerk bei der ersten Anmeldung als „Öffentlich“ deklariert wird.

Das Tor zum **Internet**

Die meisten Telekommunikationsdienstleister bieten ihren Kunden Router an, mit denen diese ihre Endgeräte in das Internet einbinden können (DSL-Router). Aber auch kleine Heimnetzwerke können durch diese kleinen Schaltzentralen eingerichtet werden. Häufig besitzen Router auch eine eingebaute Hardware Firewall, die die Netzwerknutzer vor Angriffen von außen schützt.

Wichtig ist, dass die Konfigurationsoberfläche Ihres Routers durch ein individuelles Passwort gesichert wird, d. h. ändern Sie so schnell wie möglich das Passwort, das der Hersteller vergibt. Denn dieses ist auch Cyber-Kriminellen bekannt und wird bei Angriffen bevorzugt verwendet.

Angriffe auf Router führten beispielsweise dazu, dass statt der legitimen Bank-Website betrügerische Phishing-Webseiten aufgerufen wurden, was für den Nutzer nicht erkennbar ist. In anderen Fällen gliedern Kriminelle den Router in ein Botnetz ein, um zum Beispiel eine Masse an Spam-Mails zu versenden. Außerdem ist der Router der Eingang in das lokale Netzwerk, wodurch die Dateien auf einem Netzwerkrechner bei einem unsicheren Router nicht geschützt sind.

Voreingestellte Verschlüsselungsverfahren nutzen
Basierend auf einer asymmetrischen Verschlüsselung stellen die Verfahren WPA2 und AES sichere Technologien zur Datenübermittlung zwischen den eingebundenen Geräten zum Router dar.

Über Ihren WLAN-Router lassen sich Gästenetzwerke einrichten. Um Ihr Netzwerk ausreichend zu schützen, richten Sie ein zweites Netzwerk für Ihre Gäste sowie wenn möglich für IoT-Geräte ein, und versehen dies mit einem separaten WPA2-Passwort.

Unsere Tipps für Ihren Schutz

- Stellen Sie sicher, dass auf dem Router durch regelmäßige **Updates** die aktuelle Firmware installiert ist und achten Sie darauf, dass die automatische Update-Funktion aktiviert wurde.
- Darüber hinaus sichern Sie Ihre WLAN-Router mit einem mindestens 16 Zeichen langen **Passwort.**
- Stellen Sie als **Verschlüsselung** ausschließlich WPA2 mit AES ein (auch „WPA2 only/AES“ oder „WPA2CCMP“), um Ihre Daten sorgfältig zu verschlüsseln.
- Die Vergangenheit hat gezeigt, dass **Komfortfunktionen** wie **WPS** zum automatischen Einloggen angreifbar waren. Wenn möglich, schalten Sie diese über das Webinterface des Routers aus.

Das BSI hat einen Standard entwickelt, um die Sicherheit von Routern zu gewährleisten. Zukünftig können sich Hersteller nach diesem Standard zertifizieren lassen.

Die **Zukunft** klingelt schon

Das Smart Home klingt wie ein Versprechen der Zukunft: Wohn- und Lebensqualität, aber auch Sicherheit sollen erhöht werden, die Energienutzung wird effizienter, die Wohnung stellt sich ganz auf Ihre Bedürfnisse ein.

Tatsächlich sind inzwischen die technischen Grundlagen geschaffen, um diesen futuristischen Traum in die Gegenwart zu holen. Das Internet der Dinge führt dazu, dass sich alles im Haushalt vernetzt und durch Schnittstellen aus dem Internet heraus steuern lässt. Dies kann durch die Bewohner, aber auch durch andere technische Geräte geschehen. Die Verknüpfung einzelner Gegenstände im Gebäude und deren Vernetzung zu dem für den Nutzer angenehmsten Erlebnis verspricht einen hohen Komfort. Doch auch hierbei sollte die Sicherheit nicht vernachlässigt werden.

Auch in der Zukunft des Smart Homes gelten die bekannten Sicherheitstipps

Da die voreingestellten Gerätepasswörter vom Hersteller oftmals bei allen Geräten identisch sind oder leicht ermittelt werden können, sollte der Nutzer diese vor der Verwendung unbedingt ändern. Gerne werden solche Geräte durch Kriminelle missbraucht und stellen damit eine Gefahr für Sie und andere dar.

Firmware-Updates auf Smart-Home-Geräten sollen sicherstellen, dass bekannte Sicherheitslücken geschlossen werden. Achten sie darauf, dass automatische Firmware-Updates auf Ihrem Gerät aktiviert sind, um die aktuelle Software des Herstellers zu nutzen.

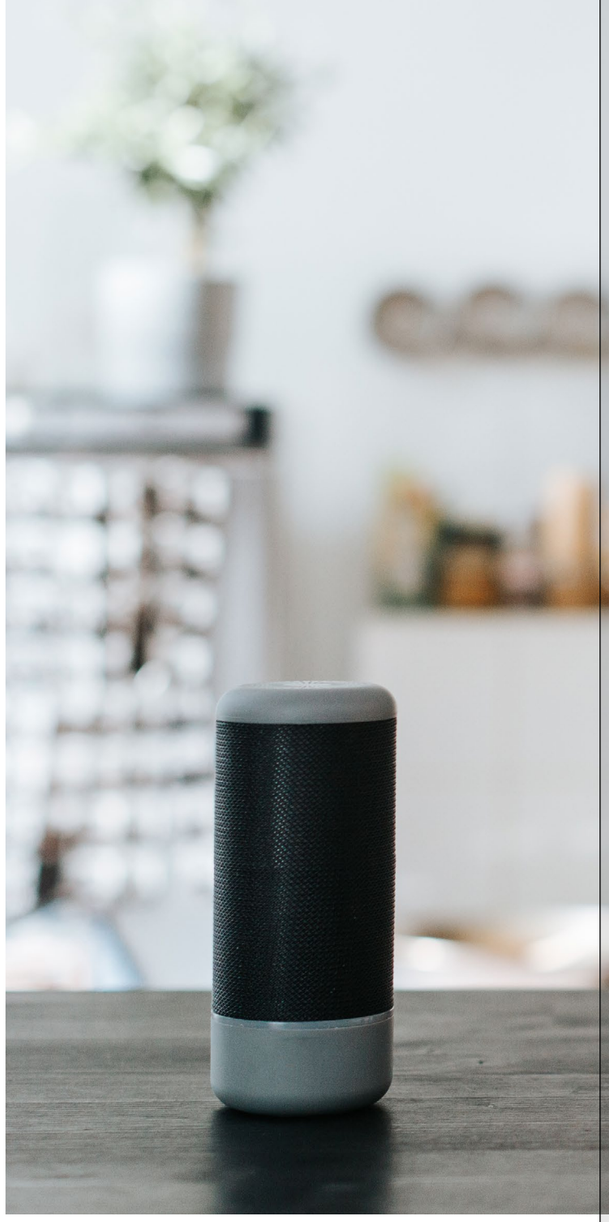
Unsere Tipps für Ihren Schutz

- **Funkstrecken** sind oftmals anfällig für Störungen, weshalb die Vernetzung von Smart-Home-Geräten wie Alarmanlagen und Kameras möglichst per Kabel erfolgen sollte.
- Schalten Sie nach Möglichkeit die Übermittlung von Daten zu Ihrem **Nutzerverhalten** ab.
- Smart-Home-Geräte ermöglichen dem Nutzer den **Fernzugriff** auf verschiedene Funktionalitäten. Nutzen Sie die vom Hersteller vorgesehenen Wege für den Fernzugriff und stellen Sie sicher, dass möglichst keine Dienste der Geräte über bspw. eine Port-Weiterleitung im Router von außen zugänglich gemacht werden.

Aktuelle Entwicklungen rund um das Thema Smart Home können Sie der Themenseite von heise.de entnehmen.

Smart Speaker hören alles

Smart Speaker gehören für viele Menschen in Deutschland bereits zum Alltag. In Deutschland hat jeder 5. Haushalt bereits einen dieser intelligenten Lautsprecher im Einsatz, 73 Prozent nutzen dabei ein Gerät von Amazon. Dabei wird häufig vernachlässigt, dass Alexa und Co. dauerhaft aktiv sind und mithören, um auf das Aktivierungswort zu reagieren.



In der Vergangenheit wurde bekannt, dass Mitarbeiter die Aufnahmen von Smart Speakern mithören, mit der Rechtfertigung durch die Datenanalyse eine stetige Verbesserung des Service gewährleisten zu wollen. Häufig sind die Smart Speaker noch mit anderen IoT-Geräten* verbunden. Dadurch lassen sich bspw. Türen öffnen oder ganze Botnetze (Fernsteuerung von IT-Systemen, um diese für bestimmte Aktionen zu missbrauchen) erschaffen, die in krimineller Absicht ferngesteuert werden können. Grundsätzlich sind alle internetfähigen Geräte – insbesondere im Smart-Home-Bereich – potentielle Ziele für Cyber-Kriminelle. Ganz verzichten muss man auf Smart Speaker oder andere IoT-Geräte nicht, da diese auch längst in der Gesellschaft angekommen sind.

Um den Sicherheitsrisiken vorzubeugen werden nachfolgend einige hilfreiche Tipps zum Umgang mit Smart-Speakern gegeben.

- Smarte Geräte in einem eigenen Heimnetzwerk betreiben um andere Geräte zu schützen
- Eine PIN oder ein sicheres Passwort für die Sprachsteuerung
- Aufgezeichnete Befehle regelmäßig im Benutzerprofil überprüfen und Auffälligkeiten löschen.
- Keine sensiblen Daten wie etwa Passwörter vor dem Sprachassistenten erwähnen
- Smart Speaker abschalten, wenn er nicht länger genutzt wird.

*IoT = Beim dem Internet of Things (dt. Internet der Dinge) handelt es sich um physische Geräte (Things), die in ein Netzwerk eingebunden sind und mit Sensoren, Software und anderer Technik ausgestattet sind. Diese können sich dadurch mit anderen Geräten und Systemen über das Internet vernetzen und Daten untereinander austauschen.

Quellenangabe: www.spiegel.de

Social Engineering

Als Social Engieering wird eine Angriffsmethode von Hackern bezeichnet. Diese versucht unter nichttechnischen, also sozialen Methoden persönliche Informationen wie Passörter oder Zugangsdaten zum Online-Banking von potenziellen Opfern zu erlangen. Diese Methode findet sowohl im privaten als auch im geschäftlichen Umfeld immer häufiger Anwendung. Dabei wird in fünf Arten des Social Engineerings unterschieden:

1. Spear Phishing

Im Gegensatz zu den meisten Phishing-Kampagnen zielt das Spear Phising auf spezielle Zielgruppen ab. Diese Spear Phishing Kampagnen nutzen oft Informationen aus Social Media Kanälen. Dabei treten die Hacker in den E-Mails als Freunde, Bekannte oder Geschäftspartner auf. Sie versuchen dadurch eine Verbindung mit dem Opfer herzustellen und einen persönlichen Kontakt zu schaffen. Der Hintergrund ist analog der Phishing-Kampagnen, auf bspw. das Klicken auf einen Link zu verseuchten Internetseiten oder schadhaften Downloads.

2. Baiting

Das sog. Baiting (Ködern) enthält eine physische Komponente in Form bspw. eines infizierten USB-Sticks. Das Ziel dabei ist, das Opfer zu manipulieren, dass es USB-Stick an den Computer anschließt. Die Köder werden oftmals an Schreibtischen von Opfern mit Aufschriften wie „wichtig“ oder „vertraulich“ deponiert, in der Hoffnung, dass das Opfer den Köder nimmt. Sobald das Opfer den USB-Stick in den Computer steckt, wird der Rechner und ggf. das gesamte Netzwerk infiziert.

3. Pretexting

Beim Pretexting wird durch die Verwendung eines fesselnden Vorwands die Aufmerksamkeit des Zielopfers erzeugt. Dadurch wird durch den Hacker versucht wertvolle Informationen von seinem Opfer zu erhalten. Hier sind als eine sehr geläufige Attacke, die sog. nigerianischen E-Mail-Scams zu nennen. Bei diesen wird den Opfern viel Geld versprochen wird, wenn diese ihre Kontaktinformationen preisgeben.

4. Contact Spamming

Bei dieser Methode werden Spam-Nachrichten an alle Kontakte des Opfers gesendet, entweder per E-Mail oder auch in den Social Media Kanälen. Die E-Mails werden von dem gehackten Benutzerkonto des Opfers verschickt. Sie sehen daher sehr realistisch aus und landen seltener im Spam-Ordner des Posteingangs. Der Freund des Opfers erhält bei dieser Methode eine E-Mail mit einem Link, den er Anklicken soll. Mit dem Klick auf dem Link, kann zum einen schädliche Software auf den Rechner des Freundes geladen werden und zum anderen eine Kopie dieser Nachricht an alle Freunde des Freundes versandt werden (Kettenbrief-Logik).

5. Quid Pro Qou

Aus dem lateinischen „einen Gefallen für einen Gefallen“ ist eine Art des Social Engineerings, bei dem ein Gefallen zwischen einem Hacker und einem Opfer ausgetauscht werden. Oftmals stellen sich die Hacker als IT-Supporttechniker vor. Diese benötigen die Anmeldedaten des Opfers, um eine wichtige Sicherheitsüberprüfung vornehmen zu können. Darüber hinaus werden die Opfer aufgefordert für den Test die Antivirensoftware auch dem Computer zu deinstallieren bzw. ein alternatives Programm zu installieren. Dadurch erhalten die Hacker Zugriff auf den Computer des Opfers und können Schadsoftware installieren und die persönlichen Daten ausspähen.

So können Sie sich schützen:

- In der Online-Umgebung weniger Vertrauen ggü. den Gesprächspartnern haben als in der Realität und ungewöhnliche Kontaktaufnahmen hinterfragen
- Bei E-Mails von Empfängern die Sie nicht kennen ggf. die Firma anrufen und nachfragen, bevor auf Links geklickt wird
- Bei privaten E-Mails oder Nachrichten in Social Media mit Links ggf. vorher den Freund mittels eines anderen Kanals (Anruf) kontaktieren
- Niemals Daten wie Kreditkartendaten, Bankverbindung, Sozialversicherungsnummer, Personal- oder Reisepassnummer angeben
- Sollten dennoch Kreditkartendaten herausgegeben werden die Sperr-Notruf-Hotline unter 116 116 kontaktieren und die Karte sperren lassen

Quellenangabe: softwarelab.org

Immer ein guter Helfer: **Der gesunde Menschenverstand.**

Auf den vorangegangenen Seiten konnten Sie viele Hinweise, Tipps und Tricks für Ihre Sicherheit im Internet finden. Doch unabhängig vom Thema zeigt sich immer: Wer kurz innehält, skeptisch bleibt und mitdenkt, dem bleiben zumeist die schlimmsten Erfahrungen im Internet erspart.

Unabhängig von Ihrem Anliegen und der Technik, sollten Sie zwei Kernregeln immer beherzigen:

Bleiben Sie misstrauisch!

Vertrauen Sie Meldungen, Nachrichten und Aufforderungen nicht blind.

Klicken Sie nicht auf jedes Angebot, auch wenn es noch so verlockend klingt. Denn auch im Internet gibt es nichts umsonst!

Viele Anbieter, die mit Preisen und Belohnungen locken, wollen nur an Ihre Daten. Manche versuchen eventuell später, Ihre Daten weiterzuverkaufen oder durch spezielle Schadsoftware an weitere Daten von Ihnen zu gelangen.

Fragen Sie nach!

- Bei merkwürdigen Nachrichten von Freunden, rufen Sie diese an und fragen Sie nach, ob die Nachricht wirklich von dem oder der Bekannten stammt.
- Haben Sie Zweifel an der Integrität einer Webseite, suchen Sie im Impressum nach einer Telefonnummer und verschaffen Sie sich telefonisch einen Eindruck von der Situation.

Auch das Team der Informationssicherheit in der apoBank steht Ihnen für Rückfragen zur Verfügung.

Weitere empfehlenswerte Seiten zur Informationssicherheit sind insbesondere www.bsi-fuer-buerger.de und die Sicherheitscheckliste von heise.de

Sicherheit im Internet

Deutsche Apotheker- und Ärztebank eG
Richard-Oskar-Mattern-Straße 6 | 40547 Düsseldorf

T 211 5998 0 | **F** 211 5938 77
M info@apobank.de | apobank.de

apoBank
Bank der Gesundheit