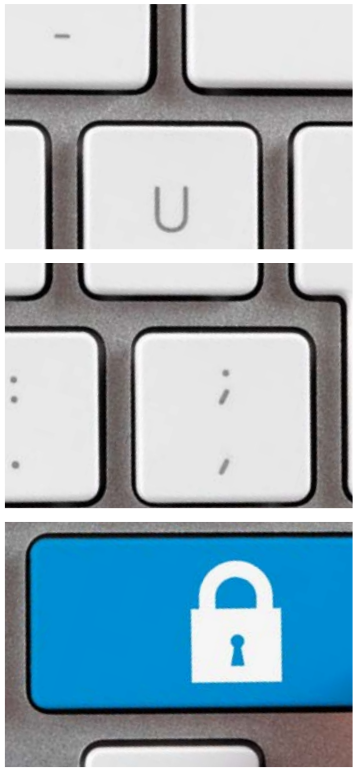
CREDIT SUISSE

Was Sie über Cybersicherheit wissen sollten

Inhalte



Cybersicherheit

Für die Credit Suisse steht die Sicherheit Ihrer Informationen stets an erster Stelle. Wir arbeiten beständig daran, unsere Systeme, Software, Netzwerke und sonstigen technologischen Komponenten vor unbefugtem Zugriff durch Dritte zu schützen, die vertrauliche Daten abrufen oder löschen, unseren Geschäftsbetrieb stören oder sonstige Schäden anrichten wollen.

Spezialisierte Mitarbeitende in aller Welt konzentrieren sich rund um die Uhr auf die Wahrung unserer Cybersicherheit und arbeiten dabei mit Regulierungsbehörden, Strafverfolgungsbehörden und anderen Unternehmen zusammen, um unsere Verteidigung und unsere Widerstandsfähigkeit gegen Bedrohungen zu stärken.

Die Entwicklung der Technologie schreitet mit immer grösseren Schritten voran, und längst ist unsere Welt geprägt von sozialen Netzwerken, Online-Transaktionen, Cloud-Computing und automatisierten Prozessen. Doch mit dem technischen Fortschritt entwickelt sich auch die **Cyberkriminalität** weiter. Ständig werden neue Angriffsarten, Tools und Methoden entwickelt, mit denen Kriminelle in zunehmend komplexere und besser kontrollierte Umgebungen eindringen und dort immer gewaltigere Schäden anrichten können – manchmal sogar, ohne dass man ihre Spuren zurückverfolgen kann.

Auch für Sie ist das Internet aller Wahrscheinlichkeit nach ein wichtiger Bestandteil Ihres alltäglichen Lebens, doch entsprechend wächst die Gefahr, Opfer eines Cyberangriffs zu werden. Deshalb ist es für uns alle **unerlässlich**, Betrugsprävention fest im Alltag zu verankern.

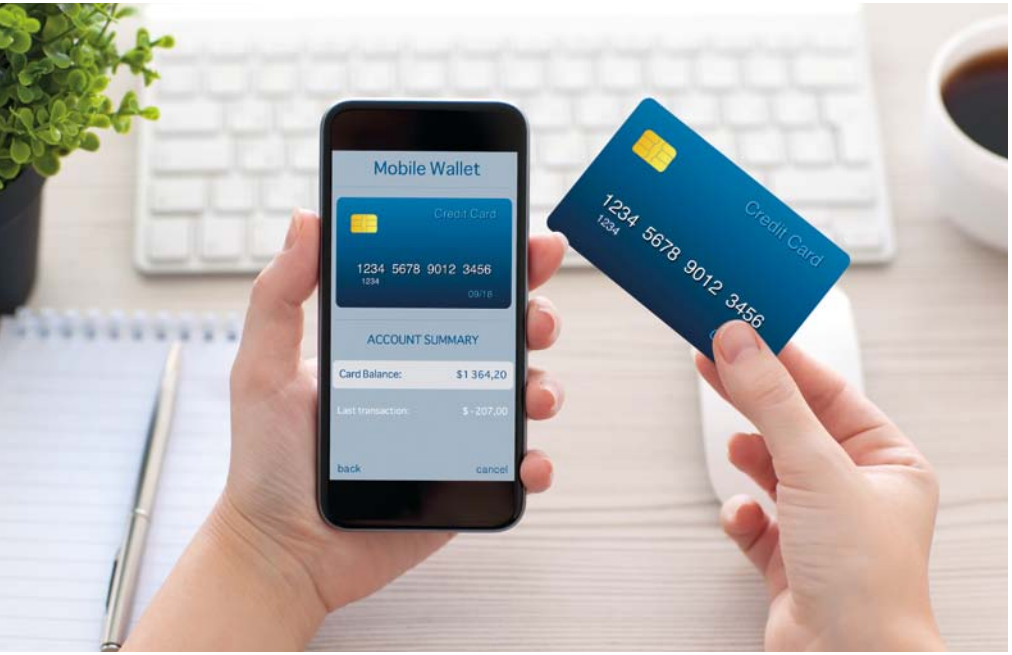
Mit dieser Informationsbroschüre möchten wir Sie daran erinnern, wie Sie sich selbst, Ihre Vermögenswerte und Ihre persönlichen Daten vor Online-Betrügern schützen können.

Ihre Cybersicherheits-Checkliste

Ein paar Tipps zum Schutz Ihrer Computer und Ihres Geldes vor Online-Betrügern

1. **Installieren Sie Sicherheitsprogramme, die ständig in Betrieb sind und regelmässig aktualisiert werden, um aktuelle Bedrohungen aufzuspüren.**
   Installieren Sie Antivirensoftware, um sich gegen Malware (schädliche Software) zu schützen, die Informationen wie Kontonummern und Passwörter stehlen kann, und verwenden Sie eine Firewall, um unbefugte Zugriffe auf Ihren Computer zu verhindern.

2. **Achten Sie genau darauf, wo und wie Sie sich mit dem Internet verbinden, wenn Sie online Bankdienstleistungen nutzen möchten oder aus einem anderen Grund sensible persönliche Daten weitergeben müssen.**
   Die Nutzung von öffentlichen WLAN-Netzwerken und Computern an öffentlichen Orten wie Bibliotheken oder Business Centers von Hotels kann riskant sein, wenn dort keine aktuelle Sicherheitssoftware installiert ist.



3. **Informieren Sie sich über die Standardfunktionen in Bezug auf Internetsicherheit.**
   Installieren Sie Antivirensoftware, um sich gegen Malware (schädliche Software) zu schützen, die Informationen wie Kontonummern und Passwörter stehlen kann, und verwenden Sie eine Firewall, um unbefugte Zugriffe auf Ihren Computer zu verhindern.

4. **Ignorieren Sie unerwartete E-Mails, die Sie dazu auffordern, einen Link oder Anhang zu öffnen, wenn Sie nicht sicher sind, wer Ihnen das E-Mail geschickt hat und warum.**
   Cyberkriminelle sind Meister im Fälschen von E-Mails. Fake-Mails können echt aussehen, aber die Installation von Malware bedingen. Am sichersten fahren Sie, wenn Sie unerwartete E-Mails mit einer Aufforderung zum Öffnen von Anhängen oder Links einfach ignorieren oder sich über eine Ihnen bekannte, öffentliche E-Mail-Adresse oder Telefonnummer bestätigen lassen, dass der angegebene Absender das E-Mail tatsächlich geschickt hat.

5. **Seien Sie misstrauisch, wenn jemand Sie unerwartet online kontaktiert und nach persönlichen Daten fragt.**
   Eine sichere Strategie ist das Ignorieren unerwünschter Informationsanfragen, egal, wie seriös sie erscheinen – insbesondere dann, wenn Sie nach Ihrer Sozialversicherungsnummer, nach Kontonummern oder Passwörtern gefragt werden.

6. **Nutzen Sie für Finanzkonten stets die sicherste Anmeldemöglichkeit.**
   Nutzen Sie «starke» Passwörter, die schwer zu erraten sind. Ändern Sie Ihre Passwörter häufig und vermeiden Sie es, für mehrere Konten das gleiche Passwort bzw. die gleiche PIN (Persönliche Identifikationsnummer) zu verwenden.

7. **Gehen Sie bei der Nutzung von sozialen Netzwerken diskret vor.**
   Kriminelle durchforsten Seiten nach Informationen wie Geburtsort, Mädchennamen der Mutter oder Namen von Haustieren, da diese Angaben ihnen dabei helfen können, die Passwörter für Online-Konten zu erraten oder zurückzusetzen.

8. **Seien Sie bei der Nutzung von Smartphones und Tablets vorsichtig.**
   Lassen Sie Ihr Mobilgerät nicht unbeaufsichtigt; schützen Sie es für den Fall eines Diebstahls oder Verlusts mit einem Gerätepasswort oder einer anderen Form der Zugriffskontrolle.

Persönliche Cybersicherheit auf einen Blick

Schützen Sie Ihren Computer. Installieren Sie Software, die Sie gegen Malware oder Schadsoftware schützt, die unbefugt auf Ihren Computer zugreifen und Ihre Passwörter oder Kontonummern stehlen kann. Nutzen Sie ausserdem eine Firewall, um unbefugte Zugriffe auf Ihren PC zu verhindern. Die Schutzoptionen sind unterschiedlich, doch in jedem Fall sollten Sie Einstellungen vornehmen, die eine automatische Aktualisierung ermöglichen.

Nutzen Sie für Finanzkonten stets die sicherste Anmeldemöglichkeit. Nutzen Sie stets die stärkste Authentifizierungsmethode, die Ihnen zur Verfügung steht, insbesondere bei risikoreichen Transaktionen. Wählen Sie Passwörter, die schwierig zu erraten sind, und halten Sie sie geheim. Erstellen Sie «starke» Nutzer-IDs und Passwörter für Ihre Computer, Mobilgeräte und Online-Konten, die aus einer Kombination aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen und entsprechend schwierig zu erraten sind. Denken Sie ausserdem daran, Ihre Passwörter regelmässig zu ändern. Es kann verlockend sein, einfach das gleiche Passwort oder die gleiche PIN für mehrere Konten zu verwenden, doch damit ermöglichen Sie einem Kriminellen, der ein einzelnes Passwort oder eine PIN erbeuten kann, auf mehrere Ihrer Konten zuzugreifen.

Machen Sie sich mit den verfügbaren Internetsicherheitsfunktionen vertraut. Sie können sich sicherer sein, dass eine Website echt ist und Ihre Informationen während der Übertragung verschlüsselt (Scrambling), wenn sie mit «https://» beginnt. Melden Sie sich ausserdem immer an Ihren Finanzkonten ab, wenn Sie Ihre Transaktionen abgeschlossen haben oder sich vom Computer entfernen. Weitere mögliche Sicherheitseinstellungen werden in der Nutzeranleitung zu Ihrem Webbrowser erläutert.

Misstrauen Sie unerwarteten E-Mails, die Sie dazu auffordern, einen Link anzuklicken, einen Anhang herunterzuladen oder Kontoinformationen preiszugeben. Für Cyberkriminelle ist es ein leichtes Unterfangen, das Logo eines renommierten Unternehmens oder einer vertrauenswürdigen Organisation in ein Phishing-E-Mail zu kopieren. Indem Sie auf eine einfache Anfrage reagieren, könnten Sie Malware installieren. Am sichersten ist es daher, unerwartete Anfragen zu ignorieren – ganz gleich, wie seriös oder verlockend sie auch erscheinen mögen.

Achten Sie darauf, wo und wie Sie sich mit dem Internet verbinden. Nutzen Sie für den Online-Zugriff auf Bank- oder andere Dienstleistungen, für die Sie persönliche Daten weitergeben müssen, Ihren eigenen Laptop / Ihr eigenes Mobilgerät und bekannte, vertrauenswürdige und sichere Verbindungen. Ein öffentlicher Computer, beispielsweise im Business Center eines Hotels oder in einer öffentlichen Bibliothek, und kostenlose öffentliche WLAN-Netzwerke sind nicht immer sicher. An solchen Orten haben Cyberkriminelle häufig leichtes Spiel und können den Internetverkehr anzapfen.

Gehen Sie bei der Nutzung von sozialen Netzwerken sorgfältig vor. Cyberkriminelle sammeln über soziale Netzwerke persönliche Informationen wie den Geburtsort, das Geburtsdatum, die Namen von Haustieren, den Mädchennamen der Mutter und sonstige Hinweise, die ihnen dabei helfen können, Passwörter zu erraten oder zurückzusetzen.

Gewähren Sie niemandem, den Sie nicht kennen und dem Sie nicht vertrauen, Zugriff auf Ihre Seite oder Ihre Informationen. Cyberkriminelle können sich als «Freunde» ausgeben, um Sie davon zu überzeugen, Ihnen Geld zu schicken oder persönliche Informationen preiszugeben.

Treffen Sie in Bezug auf Ihr Tablet oder Smartphone Sicherheitsvorkehrungen. Ziehen Sie in Betracht, die Option zur automatischen Aktualisierung des Betriebssystems und der «Apps» (Anwendungen) Ihres Geräts bei Verfügbarkeit entsprechender Software-Updates zu aktivieren, um Ihre Anfälligkeit für Sicherheitslücken in Ihrer Software zu verringern. Lassen Sie Ihr Mobilgerät nicht unbeaufsichtigt; schützen Sie es für den Fall eines Diebstahls oder Verlusts mit einem Gerätepasswort oder einer anderen Form der Zugriffskontrolle. Aktivieren Sie die Zeitüberschreitungs- oder automatische Sperrfunktion, um Ihr Gerät zu schützen, wenn es eine gewisse Zeit lang nicht verwendet wird. Informieren Sie sich immer gründlich über Apps, bevor Sie sie herunterladen.

Geschäftliche Cybersicherheit auf einen Blick

Schützen Sie Computer und Netzwerke. Installieren Sie Sicherheits- und Antivirensoftware, die Sie vor Malware oder Schadsoftware schützt, die unbefugt auf Ihr System zugreifen und dort auf verschiedene Weise Schaden anrichten kann – unter anderem durch Informationsdiebstahl. Verwenden Sie ausserdem eine Firewall, die Sie gegen unbefugten Zugriff abschirmt. Da es unterschiedliche Schutzoptionen gibt, gilt es, eine zu finden, die der Grösse und Komplexität Ihres Unternehmens Rechnung trägt. Aktualisieren Sie die Software so oft wie nötig, damit sie aktuell bleibt. Sie können die Antivirensoftware beispielsweise so einrichten, dass nach jeder Aktualisierung eine Prüfung durchgeführt wird. Wenn Sie ein drahtloses Netzwerk (WLAN) verwenden, müssen Sie sicherstellen, dass es geschützt und verschlüsselt ist. Richten Sie starke Passwörter ein, um den Router vor unbefugtem Zugriff zu schützen.

Machen Sie eine starke Authentifizierung zur Voraussetzung. Stellen Sie sicher, dass Mitarbeitende und andere Nutzer, die sich mit Ihrem Netzwerk verbinden, «starke» Nutzer-IDs und Passwörter für ihre Computer, Mobilgeräte und Online-Konten einrichten, die aus einer Kombination aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen und entsprechend schwierig zu erraten sind. Denken Sie ausserdem daran, dass Passwörter regelmässig geändert werden sollten. Ziehen Sie eine Multi-Faktor-Authentifizierung in Betracht, bei der neben einem Passwort weitere Angaben für einen Zugriff erforderlich sind. Informieren Sie sich bei Anbietern, die sich auf den Umgang mit sensiblen Daten spezialisiert haben, ob sie Multi-Faktor-Authentifizierungslösungen für den Zugriff auf Systeme oder Konten anbieten.

Kontrollieren Sie den Zugriff auf Daten und Computer und erstellen Sie Nutzerkonten für alle Mitarbeitenden. Treffen Sie Vorkehrungen, um den Zugriff auf oder die Nutzung Ihrer Computer auf autorisierte Personen zu beschränken. Schliessen Sie alle Laptops sicher ein, wenn sie nicht verwendet werden, da sie leicht verloren gehen oder gestohlen werden können. Verpflichten Sie alle Mitarbeitenden zur Nutzung eines separaten Nutzerkontos und verbieten Sie gemeinsame Konten. Gewähren Sie Ihren Mitarbeitenden nur auf die Datensysteme Zugriff, die sie für ihre Arbeit brauchen, und erlauben Sie ihnen nicht, ohne vorherige Genehmigung Software zu installieren. Stellen Sie zudem sicher, dass Administratorenrechte ausschliesslich an Mitarbeitende vergeben werden, die sie wirklich benötigen (z.B. IT-Mitarbeitende und Personen in Schlüsselfunktionen), und überprüfen Sie regelmässig, ob diese Notwendigkeit noch besteht.

Bringen Sie den Mitarbeitenden die Grundlagen bei. Führen Sie Sicherheitspraktiken und Richtlinien für die Mitarbeitenden ein, beispielsweise zur angemessenen Nutzung des Internets; definieren Sie sowohl Erwartungen als auch Konsequenzen bei Verstössen. Etablieren Sie eine Top-down-Unternehmenskultur, die die Bedeutung von Cybersicherheit unterstreicht, insbesondere im Hinblick auf den Umgang mit und den Schutz von Kunden- und anderen wichtigen Daten. Stellen Sie sicher, dass die Mitarbeitenden wissen, wie sie potenzielle Sicherheitsverstösse erkennen und melden können. Weisen Sie die Mitarbeitenden immer wieder darauf hin, wie wichtig es ist, darauf zu achten, wo und wie sie sich

mit dem Internet verbinden. Mitarbeitende und Dritte sollten nur über eine vertrauenswürdige und sichere Verbindung auf Ihr Netzwerk zugreifen. Öffentliche Computer (beispielsweise in Internetcafés, Business Centers von Hotels oder öffentlichen Bibliotheken) sind möglicherweise nicht sicher. Ausserdem sollten sich Ihre Mitarbeitenden nicht über eine WLAN-Verbindung mit Ihrem Firmennetzwerk verbinden, die möglicherweise unsicher ist, was bei vielen kostenlosen WLAN-Netzwerken an öffentlichen «Hotspots» der Fall sein kann. An solchen Orten haben Cyberkriminelle häufig leichtes Spiel und können den Internetverkehr anzapfen.

Schulen Sie die Mitarbeitenden im Hinblick auf die Gefahren verdächtiger E-Mails. Schaffen Sie bei Ihren Mitarbeitenden ein grundsätzliches Misstrauen gegenüber unerwarteten E-Mails, die sie dazu auffordern, einen Link anzuklicken, einen Anhang herunterzuladen oder Kontoinformationen preiszugeben. Für Cyberkriminelle ist es ein leichtes Unterfangen, das Logo eines renommierten Unternehmens oder einer vertrauenswürdigen Organisation in ein Phishing-E-Mail zu kopieren. Indem Ihre Mitarbeitenden auf eine auf den ersten Blick einfache Anfrage reagieren, installieren sie möglicherweise Malware in Ihrem Netzwerk. Am sichersten ist es also, unaufgeforderte Anfragen zu ignorieren – ganz gleich, wie seriös sie auch erscheinen mögen. Softwareanbieter stellen regelmässig Patches oder Aktualisierungen für ihre Produkte zur Verfügung, um Sicherheitslücken zu schliessen und die Funktionalität zu verbessern. Am besten laden Sie diese Aktualisierungen herunter und installieren sie, sobald sie verfügbar sind. Am effizientesten ist es, die Software so einzurichten, dass sie alle verfügbaren Updates automatisch installiert.

Machen Sie Sicherungskopien wichtiger Systeme und Daten. Erstellen Sie regelmässig Backups der von Ihrem Unternehmen genutzten Computer. Ausserdem sollten Sie für Ihre Backup-Daten die gleichen Sicherheitsvorkehrungen (z. B. Verschlüsselung) wie für die Originaldaten treffen. Legen Sie neben Ihren automatischen Backups zusätzlich regelmässig Sicherungskopien sensibler Unternehmensdaten auf einem Speichergerät an einem sicheren Zweitstandort an.

Achten Sie sehr genau auf die Bewegungen auf Ihren Bankkonten, sodass Sie nicht genehmigte Abhebungen erkennen. Richten Sie zudem zusätzliche Kontrollmechanismen ein. Beispielsweise können Sie mit Ihrem Finanzinstitut vereinbaren, dass eine telefonische Bestätigung eingeholt wird, bevor eine Transaktion initiiert wird. Seit einigen Jahren kommt es immer häufiger zu nicht genehmigten elektronischen Abbuchungen von Unternehmensbankkonten. Eine häufig verwendete Betrugsmasche ist die Übernahme eines Kontos. Hierfür verwenden Cyberkriminelle beispielsweise Schadsoftware zur Tastatureingabeprotokollierung, um an die IDs und Passwörter für Online-Bankkonten zu gelangen und Geld abzuheben. Eine weitere Taktik mit der Bezeichnung «Business Email Compromise» (BEC) zielt direkt auf Unternehmen ab und beschreibt das Fälschen von Zahlungsaufforderungen. Diese sehen so aus, als seien sie von seriösen Lieferanten gesendet worden, das Transaktionsziel ist jedoch ein Konto des Cyberkriminellen. Unternehmen unterliegen in der Regel nicht dem Verbraucherschutz bei nicht autorisierten elektronischen Zahlungsverkehr.

Denken Sie auch an Tablets und Smartphones. Mobilgeräte können Ihre Sicherheit ernsthaft gefährden, besonders, wenn sich darauf vertrauliche Informationen befinden oder damit der Zugriff auf das Netzwerk Ihres Unternehmens möglich ist. Wenn sich Ihre Mitarbeitenden mit ihren Geräten mit dem Unternehmensnetzwerk verbinden, sollten Sie sie dazu verpflichten, einen Passwortschutz für ihre Geräte einzurichten, ihre Daten zu verschlüsseln und Sicherheitsapps zu installieren, die Kriminelle daran hindern, auf die Geräte zuzugreifen, wenn sie mit öffentlichen Netzwerken verbunden sind. Ausserdem sollten Sie Meldeverfahren für verlorengegangene oder gestohlene Geräte entwickeln und ihre Anwendung durchsetzen.

Achten Sie auf betrügerische Transaktionen und Rechnungen. Betrugsversuche reichen von Zahlungen mit wertlosen Schecks oder einer gefälschten Kredit- oder Debitkarte bis hin zu betrügerischen Warenretouren. Schliessen Sie eine Versicherung ab, die Sie gegen derartige Risiken schützt. Zudem sollten Sie allfällige Unregelmässigkeiten umgehend melden.

E-Mail

Ihr E-Mail-Anbieter kann nicht für Ihre Cybersicherheit garantieren. Hacker greifen regelmässig Anbieter an, um Zugriff auf Nutzerkonten zu erhalten, oder starten gezielte Angriffe auf individuelle Nutzerkonten und versuchen, sich mit Phishing, Social Engineering, Malware oder sonstigen Taktiken Zugang zu verschaffen.

Sie können Ihre Anfälligkeit für derartige Betrugsversuche verringern, indem Sie separate E-Mail-Konten für verschiedene Zwecke einrichten:

- Geschäftliches
- Familie und Freunde
- Wichtige Mitteilungen
- Seiten, die zur Anmeldung eine E-Mail-Adresse als Nutzerkennung erfordern

Zusätzlich können Sie zum Schutz Ihrer Informationen folgende Massnahmen ergreifen:

- Sofern verfügbar, aktivieren Sie in Ihrem E-Mail-Service die Zwei-Faktor-Authentifizierung, um eine Mitteilung zu erhalten, wenn ein Anmeldeversuch von einem anderen Computer erfolgt.
- Verschlüsseln Sie persönliche Daten für die Übertragung. Durch die Verschlüsselung wird es für andere Anwender unmöglich, die Daten ohne den Schlüssel zu lesen.
- Verwenden Sie Spamfilter, um Risiken in Verbindung mit Schadsoftware und Phishing-Versuchen zu reduzieren (Spam macht 65 % des gesamten E-Mail-Verkehrs aus).
- Wenn Sie jemandem ein passwortgeschütztes Dokument senden möchten, schicken Sie das Dokument in einem E-Mail und das Passwort in einem anderen.

Social Engineering

Social Engineering kann Sie anfällig für Betrugsversuche machen. Soziale Netzwerke wie Facebook oder LinkedIn stellen Hackern eine Fülle an Informationen über Sie zur Verfügung, die sie verwenden können, um Ihre Daten oder Vermögenswerte zu stehlen.

- Geben Sie online nicht zu viele Informationen preis. Kriminelle durchsuchen Facebook, Twitter und andere soziale Medien, um Informationen über Sie zu finden und diese für Betrugsversuche gegen Sie, Ihre Familie und/oder Ihre Freunde zu nutzen.
- Versenden Sie keine persönlichen oder finanziellen Informationen in E-Mails; folgen Sie keinen Links, die Ihnen zugeschickt werden – selbst, wenn sie aus vertrauenswürdigen Quellen zu stammen scheinen.
- Kontaktieren Sie bei einem verdächtigen E-Mail den Absender zunächst telefonisch oder öffnen Sie ein neues E-Mail-Fenster (klicken Sie keinesfalls auf «Antworten»), um den Absender zu fragen, ob das E-Mail, das Sie erhalten haben, tatsächlich sicher ist.
- Achten Sie auf die URL. Schädliche Websites sehen echten Websites täuschend ähnlich, die URL kann jedoch Schreibvarianten oder eine andere Domain enthalten (beispielsweise «.net», wenn es eigentlich «.com» sein sollte).
- Geben Sie auf Websites keine sensiblen Informationen ein, wenn die Website nicht gesichert ist. Gesicherte URLs beginnen mit «https://».

Telefonisch

Prüfen Sie die Identität unbekannter Anrufer: Fragen Sie nach dem vollständigen Namen und der korrekten Schreibweise des Namens, nach einer Rückrufnummer und einer Begründung für die Informationsanfrage.

Hüten Sie sich vor Hochstaplern: Überprüfen Sie Anrufer mittels offizieller, öffentlicher Kanäle.

Geben Sie keine Informationen über andere Personen weiter: Fordern Sie Anrufer dazu auf, sich direkt an die betreffende Person zu wenden, wenn Sie nach Informationen über jemand anderen gefragt werden.

Persönlich

Achten Sie an öffentlichen Orten auf «Schultersurfer», die Sie dabei beobachten, wie Sie persönliche Daten wie PINs oder Passwörter eingeben, um sie zu stehlen und auf Ihre Konten zuzugreifen.

- Achten Sie beim Betreten eines Sicherheitsbereichs auf Menschen, die den Bereich gemeinsam mit Ihnen betreten, ohne eine eigene Autorisierung (z. B. einen Ausweis oder ein Token) zu verwenden.
- Schliessen Sie keine unbekannten Speichergeräte wie USB-Sticks, die Sie gefunden haben oder die Ihnen gegeben wurden, an Computer an – sie könnten Malware enthalten.

Online

Hacker erstellen Kopien bekannter Websites, um Ihre Nutzerdaten (Passwörter, Sozialversicherungsnummer, Kreditkarteninformationen usw.) zu erbeuten. Mit diesen gestohlenen Informationen greifen sie anschliessend auf Ihre Bank- und sonstigen Konten zu.

Vorsichtsmassnahmen bei der Internetnutzung:

- Verwenden Sie stets die aktuelle Softwareversion Ihres Browsers.
- Setzen Sie die Sicherheitseinstellungen Ihres Browsers mindestens auf eine mittlere, besser noch auf eine hohe Stufe.
- Vergewissern Sie sich, dass die Webadressen der Seiten, die Sie besuchen, mit «https://» beginnen. Manche Browser zeigen neben dem «https://» ein Sicherheitsschloss-Symbol an, um zu verdeutlichen, dass die Verbindung sicher ist.
- Denken Sie immer daran: «http://» ist nicht sicher.
- Melden Sie sich nach dem Online-Banking oder der Nutzung eines E-Commerce-Services ab, um zu gewährleisten, dass Ihre Sitzung geschlossen wurde.
- Löschen Sie Ihre Cookies und leeren Sie Ihren Browsercache, damit Hacker keinen Zugriff auf Ihren Verlauf bekommen und daraus Informationen beziehen können.
- Denken Sie daran, dass Hacker zunehmend Kinder in sozialen Netzwerken und auf Gaming-Websites ins Visier nehmen.
- Überlegen Sie sich gut, welche Seiten Sie besuchen: Rufen Sie keine Seiten auf, die illegale Downloads oder sonstige illegale Inhalte (z.B. Filesharing) anbieten: Selbst wenn Sie keine Dateien herunterladen, können Sie sich Viren einfangen, die Ihren Computer infizieren.
- Blockieren Sie Pop-ups und Werbung und reagieren Sie niemals auf Pop-ups, die Sie zur Eingabe oder erneuten Eingabe Ihrer Anmeldeinformationen auffordern.

Best-Practice-Methoden

- Prüfen Sie regelmässig den Transaktionsverlauf Ihrer Konten und Kreditkarten sowie Ihre Kontoauszüge auf verdächtige Transaktionen.
- Nutzen Sie zweistufige Authentifizierungsverfahren, wo immer sie verfügbar sind. Ein Beispiel für ein solches Verfahren ist die alltägliche Nutzung von Geldautomaten: Sie bestätigen Ihre Identität mit Ihrer Debitkarte und einer PIN. Das Gleiche sollten Sie auch online tun: Verwenden Sie für den Zugriff auf Ihr Konto ein Passwort und einen Code, den Sie per Textnachricht, E-Mail oder Anruf erhalten. Sie erhalten eine Mitteilung, falls sich jemand von einem anderen Computer aus anmeldet.
- Vermeiden Sie es, auf die «Schliessen»-Schaltfläche oder andere Elemente einer Werbeanzeige zu klicken, um sie zu schliessen.
- Verwenden Sie so oft wie möglich den «privaten» Modus Ihres Browsers, damit keine Cookies und kein Browserverlauf auf Ihrem Gerät gespeichert werden.
- Verwenden Sie für wichtige Seiten vertrauenswürdige Lesezeichen und keine E-Mail-Links oder Pop-ups.
- Schliessen Sie Fenster mit Pop-up-Anzeigen oder unerwarteten Warnungen über das X am oberen rechten Rand.
- Kaufen Sie nichts, das in einer Spam-Nachricht angepriesen wird – selbst wenn es sich um ein seriöses Unternehmen handelt, fördern Sie somit den Versand von Spam-Nachrichten.

Denken Sie daran, dass jedes Gerät Risiken birgt.

Laptops, Tablets und Mobiltelefone sind allesamt anfällig für WLAN-Sicherheitslücken. Rufen Sie keine Seiten auf, die Sie nicht kennen bzw. mit denen Sie nicht vertraut sind. Gehen Sie nicht davon aus, dass WLAN-Verbindungen seriös sind – Hacker erstellen gefälschte Zugriffspunkte, die den Anschein geben, legitim zu sein.

Verwenden Sie stattdessen ein Virtual Private Network (VPN), das nur autorisierten Nutzern den Zugriff auf Ihr Netzwerk gestattet, sodass der Datenverkehr nicht abgefangen werden kann. Rufen Sie keine Seiten auf, die Sie nicht kennen bzw. mit denen Sie nicht vertraut sind.

Sicherheit von Mobilgeräten

Im Hinblick auf Bankgeschäfte, Einkäufe und die soziale Vernetzung werden wir immer abhängiger von unseren Smartphones und Tablets. Deshalb ist es unbedingt erforderlich, dass wir unsere Mobilgeräte schützen. Wir alle sollten bestimmte Sicherheitsvorkehrungen treffen, um zu gewährleisten, dass diese Geräte geschützt sind.

Best Practices für Ihre persönlichen Geräte

- Richten Sie Ihre Sicherheitseinstellungen so ein, dass der Zugriff Dritter auf Ihre Daten über WLAN- und Bluetooth-Verbindungen beschränkt wird.
- Klicken Sie nicht auf Werbeanzeigen im Internet: Sowohl für Android- als auch für Apple-Geräte gibt es leistungsfähige Ad-Blocker-Apps, und Ihre Browsereinstellungen können angepasst werden, um Ad-Tracking zu begrenzen.
- Aktualisieren Sie die Apps auf Ihrem Gerät, sobald neue Versionen verfügbar sind, da diese oft Sicherheitslücken schliessen.
- Falls Sie denken, dass Ihr Gerät mit Malware infiziert wurde: Bitten Sie den Hersteller Ihres Geräts oder Ihren Mobilfunkanbieter um Hilfe.
- Installieren Sie eine Sicherheitsapp, die Ihr Gerät nach mit Malware infizierten Apps scannt und diese entfernt.
- Versuchen Sie nicht, die Sicherheitsvorkehrungen im Betriebssystem Ihres Geräts zu umgehen (z.B. durch einen Jailbreak oder das Rooten Ihres Mobilgeräts).
- Achten Sie darauf, dass Ihr Handy oder Computer immer gesperrt bzw. PIN-/passwortgeschützt ist.
- Aktualisieren Sie regelmässig die Systemsoftware Ihres Geräts und achten Sie darauf, dass immer die aktuellsten Sicherheitspatches installiert sind.
- Verschlüsseln Sie sensible Daten. Wenn Ihr Mobilgerät oder Laptop über Datenverschlüsselungsfunktionen verfügt, nutzen Sie diese.
- Beobachten Sie das Verhalten von Apps auf Ihrem Handy und die Zugriffsrechte/-anfragen von auf Ihrem Gerät installierten Apps.
- Verwenden Sie ein namhaftes Antiviren-/Anti-Malware-Programm und aktualisieren Sie es regelmässig. Mobilgeräte sind anfällig für die gleichen Risiken wie Heim- oder Bürocomputer.
- Deaktivieren Sie Bluetooth, wenn Sie die Verbindung gerade nicht benötigen. Ihr Gerät wird dadurch weniger anfällig für Cyberangriffe und Ihr Akku hält länger.
- Entscheiden Sie sich für ein Smartphone mit Anti-Diebstahl-Funktionen. Sollten Sie per Fernzugriff auf Ihr Handy zugreifen können, können Sie es sperren, die darauf enthaltenen Daten löschen und es orten, falls es verloren geht oder gestohlen wird.
- Erstellen Sie regelmässig Backups Ihrer Geräte auf Ihrem Heimcomputer oder in einem Cloud-Netzwerk, damit Sie auch im Falle eines Diebstahls, Verlustes oder einer Beschädigung auf Ihre Daten zugreifen können.

- Kriminelle nutzen Malware, um Daten zu stehlen oder zu zerstören und gefährden damit die Sicherheit und Integrität der von Ihnen genutzten Geräte und/oder Systeme. Ignorieren Sie Warnhinweise nicht. Installieren Sie Antivirensoftware und beachten Sie die Warnhinweise, die Sie erhalten, wenn Sie auf unsichere Seiten im Internet zugreifen.
- Überlegen Sie sich gut, was Sie anklicken und herunterladen. Wenn Sie unbekannte Links anklicken, können Sie sich dadurch Schadsoftware einfangen, die Ihren Computer scannt oder Ihre Tastatureingaben protokolliert und so Ihre Passwörter und Kontonummern abfängt.
- Einige Programme verfolgen die klare Absicht, Systeme mit Malware zu infizieren. Achten Sie bei der Installation auf die Mitteilungen, die Sie erhalten, sowie auf das Kleingedruckte. Brechen Sie die Installation umgehend ab, wenn Sie glauben, dass es sich um schädliche Software handelt.
- Achten Sie auf verdächtig aussehende E-Mails. Selbst E-Mails von Bekannten können Malware-Links oder schädliche Anhänge enthalten, wenn ihre Konten von Dritten missbraucht wurden.
- Folgen Sie Links in eingehenden E-Mails nicht, ohne sie vorher zu prüfen. Rufen Sie Websites durch die direkte Eingabe der Adresse in Ihren Browser auf, wann immer es möglich ist.
- Scannen Sie Dateien vor dem Öffnen mit Sicherheitssoftware. Gehen Sie nicht davon aus, dass per E-Mail erhaltene oder auf USB- und Flash-Speichergeräten befindliche Dateien, die Sie erhalten haben, automatisch sicher sind.

Malware

Schenken Sie Pop-up-Fenstern, die Sie dazu auffordern, Software herunterzuladen, kein Vertrauen. Ihr Ziel ist es, Sie davon zu überzeugen, dass Ihr Computer infiziert wurde und das Problem durch das Herunterladen der Software behoben werden kann. Schliessen Sie solche Fenster umgehend, achten Sie jedoch darauf, nichts innerhalb des Pop-up-Fensters anzuklicken.

- Die meisten Filesharing-Seiten sind illegal, halten Sie sich daher am besten davon fern. Auf diesen Seiten wird kaum nach Malware geprüft. Malware kann als beliebter Film, populäres Album oder Software daherkommen.
- Sollte Ihr Computer von einem Ransomware-Virus befallen werden, der Sie über ein Pop-up-Fenster darüber informiert, dass Ihre Dateien verschlüsselt wurden und Sie ein Lösegeld für ihre Entsperrung zahlen sollen, geraten Sie nicht in Panik. Unterbrechen Sie umgehend die Netzwerkverbindung des Geräts und stellen Sie die Dateien mit einem sauberen Backup, das Sie vorher angelegt haben, wieder her. Zahlen Sie auf keinen Fall Lösegeld.

Notizen

CREDIT SUISSE AG
Postfach 100
CH-8070 Zürich
credit-suisse.com

MCIZ 1 01.2018