5 Schritte für Ihre digitale Sicherheit

Ihre Polizei und die Schweizerische Kriminalprävention (SKP) – eine interkantonale Fachstelle der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)

5 Schritte für Ihre digitale Sicherheit

Das Internet ist zu einem bedeutenden Bestandteil unseres Alltags geworden. Im Internet lesen wir die neuesten Nachrichten, rufen Fahrpläne ab, bezahlen Rechnungen oder kommunizieren einfach mit Freunden und Bekannten.

Neben all diesen Möglichkeiten hat uns das Internet aber auch neue Gefahren gebracht: Unzählige Schädlinge versuchen ständig, neue Wege in unsere Computer, Smartphones oder Tablets zu finden, auf denen persönliche Daten wie Fotos, Briefe oder wichtige Dokumente gespeichert sind. Bei einem erfolgreichen Angriff können Kriminelle Ihren Geräten und Ihnen selbst einen grossen Schaden zufügen. Daten könnten verändert, gelöscht oder die darin enthaltenen Informationen missbräuchlich verwendet werden, um beispielsweise in Ihrem Namen und auf Ihre Kosten im Internet einzukaufen.

Schützen Sie deshalb Ihre Daten und Geräte mit den «5 Schritten für Ihre digitale Sicherheit»:

Schritt 1 **Sichern** der Daten

Schritt 2 **Überwachen** mit Virenschutz und Firewall

Schritt 3 **Vorbeugen** mit Software-Updates

Schritt 4 **Schützen** der Online-Zugänge

Schritt 5 **Aufpassen** und wachsam sein

Mit Sicherheitsgurt beim Crash gerettet!
Mit Datensicherung vor Datenverlust bewahrt!

1

Sichern der Daten

Wie viel sind Ihnen Ihre Daten wert? Sichern Sie diese regelmässig auf mindestens einem zweiten Medium und überprüfen Sie, ob Ihre Daten tatsächlich gespeichert worden sind.

Wichtige Merkpunkte

- Sichern Sie Ihre Daten regelmässig auf einer externen Festplatte, DVD, CD oder online in einem Cloud-Speicher.
- Prüfen Sie, ob die Daten im Backup enthalten sind und wiederhergestellt werden können.
- Schliessen Sie eine externe Sicherungsfestplatte nur bei Gebrauch an und verbinden Sie Ihren Online-Speicher für das Backup nur für den Sicherungsvorgang und nicht permanent.

Heutzutage werden auf Computern, Tablets und Smartphones grosse Mengen von Textdokumenten, E-Mails, Fotos, Videos, Musik und vieles mehr in Form von digitalen Daten gespeichert. Es ist nicht auszuschliessen, dass diese Inhalte durch Fehlmanipulation (z. B. versehentliches Löschen), wegen eines technischen Defekts (z. B. durch einen Defekt der Festplatte), durch Verlust oder Diebstahl des Geräts oder durch Schadsoftware (Viren, Würmer, Trojaner etc.) teilweise oder gar komplett verloren gehen.

→ Sichern Sie Ihre Daten mit einem Backup, bevor Sie einen Datenverlust erleiden!

Weitere Informationen mit detaillierten Anleitungen und Tools finden Sie unter:

www.ebas.ch/step1

Mit Cockpit alles unter Kontrolle!
Mit Virenschutz und Firewall den Datenverkehr überwacht!

2

Überwachen mit Virenschutz und Firewall

Welche «Zugangstüren» sind auf Ihrem Gerät offen und welche Viren gelangen darauf? Praktisch keine, wenn Sie eine Firewall aktiviert und ein Virenschutzprogramm installiert haben.

Wichtige Merkpunkte

- Nutzen Sie ein Virenschutzprogramm und aktivieren Sie dessen automatische Update-Funktion.
- Prüfen Sie Ihr Gerät regelmässig auf Schädlingsbefall, indem Sie eine vollständige Systemprüfung durchführen.
- Aktivieren Sie in Windows oder macOS die eingebaute Firewall, bevor Sie Ihr Gerät mit dem Internet oder einem anderen Netzwerk verbinden.

Ohne spezielle Massnahmen ist ein Computer, ein Tablet oder ein Smartphone den Gefahren aus dem Internet schutzlos ausgeliefert und unter Umständen innert kürzester Zeit mit Schadsoftware infiziert. Sämtliche gespeicherten Daten können dann durch unbefugte Dritte eingesehen, manipuliert oder gar gelöscht werden.

→ Überwachen Sie Ihre Internet-Kommunikation mit einem Virenschutzprogramm und einer aktivierten Firewall!

Weitere Informationen mit detaillierten Anleitungen und Tools finden Sie unter:

www.ebas.ch/step2

Mit regelmässigem Service das Auto intakt!
Mit Updates alle Programme aktualisiert!

3

Vorbeugen mit Software-Updates

Wer könnte mehr für die Sicherheit Ihrer Software tun als deren Hersteller? Versorgen Sie Ihr System, Ihre Programme und alle Apps regelmässig mit den neusten Updates.

Wichtige Merkpunkte

- Installieren Sie nur nötige Programme und Apps und laden Sie diese immer von der Herstellerseite oder einem offiziellen Store herunter.
- Aktivieren Sie die automatische Update-Funktion für das Betriebssystem und alle installierten Programme und Apps.
- Verwenden Sie für den Zugang ins Internet jeweils nur die aktuellste Version des jeweiligen Browsers.

Veraltete Programme weisen oft Sicherheitslücken auf und vereinfachen es einem Angreifer, ein Gerät unter seine Kontrolle zu bringen. Software-Hersteller korrigieren solche Sicherheitslücken und stellen die Korrekturen als Programmaktualisierungen zur Verfügung.

Nur nötige Software und Apps installieren

Installieren Sie nur wirklich notwendige Programme und Apps und achten Sie darauf, dass diese aus seriöser Quelle stammen, also direkt vom Hersteller oder aus dem offiziellen Store (z. B. Apples App-Store oder Googles Play-Store).

Halten Sie Ihre Geräte aktuell

Stellen Sie sicher, dass Sie jeweils die aktuellste Version einer Software verwenden. Die Grundlage bildet ein aktualisiertes Betriebssystem. Aber auch alle anderen installierten Programme (z. B. Browser wie Firefox oder Chrome oder Adobe Acrobat Reader) müssen auf aktuellstem Stand gehalten werden.

→ Beugen Sie vor, indem Sie aktuelle Software-Updates installieren!

Weitere Informationen mit detaillierten Anleitungen und Tools finden Sie unter:

www.ebas.ch/step3

Mit Schlüssel kein Autodiebstahl!
Mit Passwort kein Datenklau!

4

Schützen der Online-Zugänge

Verschliessen Sie die Türe, wenn Sie das Haus oder die Wohnung verlassen? Schützen Sie auch Ihre Geräte und Online-Zugänge vor fremdem Zugriff.

Wichtige Merkpunkte

- Schützen Sie Ihren Computer und Ihre mobilen Geräte (Smartphones, Tablets etc.) vor unbefugtem Zugriff und sperren Sie den Bildschirm, wenn Sie nicht aktiv am Gerät arbeiten.
- Verwenden Sie sichere Passwörter (mind. 10 Zeichen lang, aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen bestehend).
- Benutzen Sie nicht überall dasselbe Passwort, sondern für verschiedene Angebote verschiedene Passwörter.
- Aktivieren Sie nach Möglichkeit die sogenannte Zwei-Faktor-Authentifizierung.

Sorgfältiger Umgang mit Passwörtern
Kurze, nicht komplexe Passwörter sind unsicher, da sie von einem Angreifer erraten werden können. Insbesondere Nachnamen, Namen von Kindern oder Haustieren, Wörter einer bekannten Sprache, Tastaturfolgen (z. B. «asdfg» oder «45678») sowie Geburtsdaten dürfen nicht verwendet werden. **Am besten eignen sich willkürliche, mindestens 10-stellige Kombinationen aus Gross- und Kleinbuchstaben sowie Ziffern und Sonderzeichen.** Verwenden Sie nicht überall dasselbe Passwort, sondern für verschiedene Angebote verschiedene Passwörter, die Sie niemandem bekanntgeben. Merken Sie sich die Passwörter oder bewahren Sie sie an einem sicheren Ort auf.

Ein sicheres Passwort zu erstellen, ist gar nicht so schwer:
Nehmen Sie einen Satz, den Sie sich gut merken können, und bilden Sie Ihr Passwort mit den jeweiligen Anfangsbuchstaben, Ziffern und Sonderzeichen:
«**M**eine **T**ochter **T**amara **h**at **a**m **19. J**anuar **G**eburtstag**!**»
So entsteht ein Passwort aus einer beliebigen Zeichenfolge, das Sie sich gut merken können: **MTTha19.JG!**

5

Aufpassen und wachsam sein

Glauben Sie alles, was Ihnen weisgemacht wird? Nehmen Sie Ihre Eigenverantwortung wahr und surfen Sie im Internet stets mit einer gesunden Portion Misstrauen.

In einem **Passwort-Manager** können Sie sämtliche Passwörter verschlüsselt abspeichern – und müssen sich dadurch nur noch ein einziges Passwort merken.

Zwei-Faktor-Authentifizierung
Zusätzlich zu einem sicheren Passwort sorgt die sogenannte Zwei-Faktor-Authentifizierung für noch mehr Sicherheit. Dabei wird beim Login zusätzlich zum ersten Sicherheitselement (meistens ein Passwort) ein zweites, unabhängiges Sicherheitselement abgefragt. Dies kann beispielsweise ein Code sein, der auf ein Mobiltelefon geschickt oder direkt auf diesem generiert wird.

→ **Schützen Sie Ihre Geräte und Online-Zugänge vor fremdem Zugriff!**

Weitere Informationen mit detaillierten Anleitungen und Tools finden Sie unter:

www.ebas.ch/step4

Wichtige Merkpunkte

- Seien Sie beim Surfen im Internet stets misstrauisch und überlegen Sie sich gut, wo und wem Sie Ihre persönlichen Informationen preisgeben.
- Finanzinstitute, Telekommunikations- und sonstige Dienstleistungsunternehmen fragen nie nach einem Passwort (weder per E-Mail, noch per Telefon) und verlangen auf diese Weise auch keinen Passwortwechsel.
- Beachten Sie bei der Verwendung von mobilen Geräten (Smartphones, Tablets) die gleichen Vorsichtsmassnahmen wie an Ihrem Computer zuhause.
- Holen Sie sich bei Unsicherheit oder Verdacht auf einen Angriff Unterstützung bei einer Fachperson.

Mit den Schritten 1 bis 4 haben Sie Ihre Geräte und Online-Zugänge technisch sehr gut abgesichert. Oft bleibt allerdings das Verhalten der Benutzerin oder des Benutzers selbst das grösste Risiko und wird so zum Ziel von Angriffen – lassen Sie deshalb stets Ihren gesunden Menschenverstand walten.

Schutz vor Phishing und Social Engineering

Beim Phishing versuchen Betrüger in E-Mails oder am Telefon Ihr Vertrauen zu gewinnen, indem sie sich z. B. als Ihr Finanzinstitut ausgeben und Sie mit einem Link auf eine Website locken, die jener Ihres Finanzinstituts ähnlich sieht. Fallen Sie darauf herein und geben Ihre Zugangsdaten ein, können Kriminielle damit Ihr Konto plündern.

Erhöhte Risiken bei mobilen Geräten

Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App notwendig. Prüfen Sie daher kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich notwendig sind, und deaktivieren Sie nach Möglichkeit alle nicht benötigten Rechte.

→ Passen Sie auf und seien Sie im Internet wachsam unterwegs!

Weitere Informationen mit detaillierten Anleitungen und Tools finden Sie unter:

www.ebas.ch/step5

Dieses Faltblatt entstand in Zusammenarbeit mit der **Hochschule Luzern** und **«eBanking – aber sicher!».**

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking aber sicher!

Über «eBanking – aber sicher!»

«eBanking – aber sicher!» ist eine unabhängige Plattform der Hochschule Luzern – Informatik, die Sie dabei unterstützt, Ihre persönliche Informationssicherheit wahrzunehmen. Auf der Website www.ebas.ch finden Interessierte praxisnahe Informationen zu notwendigen Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen.

- Hauptseite:
  https://www.ebas.ch
- Facebook-Seite:
  https://www.facebook.com/ebankingabersicher
- YouTube-Kanal:
  https://www.youtube.com/user/ebankingabersicher
- Medien-Bereich:
  https://www.ebas.ch/mediasection

Hochschule Luzern – Informatik

Die Hochschule Luzern – Informatik bietet Bachelor- und Master-Studiengänge, anwendungsorientierte Forschung und Entwicklung sowie Weiterbildungsangebote der Informatik und Wirtschaftsinformatik auf einem Campus.

- Hauptseite Departement Informatik:
  https://www.hslu.ch/informatik
- Information Security & Privacy:
  https://www.hslu.ch/forschung-information-security

Januar 2020

Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
3001 Bern

www.skppsc.ch