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 neusten 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 **Schützen** mit Virenschutzprogramm

Schritt 3 **Überwachen** dank Firewall

Schritt 4 **Vorbeugen** mit Software-Updates

Schritt 5 **Aufpassen** und wachsam sein

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

1

Sichern der Daten

Wie wertvoll sind Ihre Daten? Sichern Sie diese regelmässig auf mindestens einem zweiten Medium und kontrollieren Sie, ob Ihre Daten tatsächlich gespeichert worden sind.

Wichtige Merkpunkte

- Sichern Sie Ihre Daten regelmässig auf eine externe Festplatte, DVD, CD oder online in einem Cloud-Speicher.
- Prüfen Sie, ob die Daten im Backup enthalten sind und wiederhergestellt werden können.
- Damit Ihre Backup-Daten bestmöglich gegen Malware-Befall geschützt sind, 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 Datenmengen in Form von Textdokumenten, E-Mails, Fotos, Videos, Musik und vielem mehr gespeichert. Es ist nicht auszuschliessen, dass diese Daten durch Fehlmanipulation (z. B. versehentliches Löschen), wegen eines technischen Defekts (z. B. durch einen Defekt der Festplatte) oder durch Viren, Würmer und Trojaner teilweise oder gar komplett zerstört werden.

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

www.ebas.ch/step1

Mit Windschutzscheibe geschützt!
Mit Virenschutz frei von digitalem Ungeziefer!

2

Schützen mit Virenschutzprogramm

Welche Viren gelangen auf Ihren Computer, Ihr Tablet oder Ihr Smartphone? Praktisch keine, wenn Sie ein Virenschutzprogramm installiert haben.

Wichtige Merkpunkte

- Nutzen Sie ein aktuelles Virenschutzprogramm.
- Konfigurieren Sie das Virenschutzprogramm so, dass es sich automatisch und regelmässig aktualisiert und Sie damit auch gegen die neusten Gefahren gewappnet sind.
- Prüfen Sie Ihren Computer oder Ihr mobiles Gerät regelmässig auf Schädlingsbefall. Lassen Sie dazu das Virenschutzprogramm das komplette System scannen, indem Sie eine vollständige Systemprüfung vornehmen.

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 (Viren, Würmer, Trojaner, Malware) infiziert. Sämtliche gespeicherten Daten können dann durch unbefugte Dritte eingesehen, manipuliert oder gar gelöscht werden.

→ Schützen Sie Ihre Geräte mit einem Virenschutzprogramm!

www.ebas.ch/step2

Mit Garagentor kein Autodiebstahl!
Mit Firewall kein Datenklau!

3

Überwachen dank Firewall

Haben Sie die «Türen» Ihres Computers oder Ihrer mobilen Geräte geschlossen? Eine aktivierte Firewall schliesst diese zuverlässig und überwacht den Internetverkehr zu Ihrem Gerät.

Wichtige Merkpunkte

- Aktivieren Sie die in Ihrem Betriebssystem eingebaute Firewall unbedingt bevor Sie Ihr Gerät mit dem Internet oder einem anderen Netzwerk verbinden.
- Gewisse Onlineprogramme, wie z.B. Onlinespiele, verlangen das Öffnen von bestimmten «Zugangstüren» (Ports). Achten Sie darauf, dass Sie nur die erforderlichen Zugänge öffnen und nicht die ganze Firewall deaktivieren.

Wenn Benutzerinnen und Benutzer mit Ihrem Computer, Tablet oder Smartphone im Internet surfen, öffnen sich auf den Geräten für die Kommunikation unsichtbare «Zugangstüren» (Ports). Diese bieten eine Angriffsfläche für Attacken aus dem Internet. Eine installierte Firewall schliesst diese Türen soweit als nötig und überwacht den Datenverkehr zwischen den Geräten und dem Internet. Die Firewall alarmiert, wenn sie «verdächtigen» Netzwerkverkehr entdeckt.

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

www.ebas.ch/step3

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

4

Vorbeugen mit Software-Updates

Wer könnte mehr für die Sicherheit Ihrer Programme tun als die Hersteller all Ihrer Programme? Pflegen und versorgen Sie Ihre Programme und Apps regelmässig mit den neusten Updates. Damit sind Sie auf der sicheren Seite.

Wichtige Merkpunkte

- Aktivieren Sie die automatische Updatefunktion für alle installierten Programme und Apps – insbesondere Betriebssystem, Virenschutzprogramm, Firewall, Browser inkl. Plug-ins und Programme zum Betrachten von Dokumenten.
- Laden Sie Programme, Apps und deren Updates immer von der Herstellerseite und nicht von Drittanbietern herunter.
- Verwenden Sie für den Zugang ins Internet jeweils nur die aktuellste Version des Browsers.

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

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

www.ebas.ch/step4

Mit Verstand im Strassenverkehr!
Mit Köpfchen im Internet!

5

Aufpassen und wachsam sein

Wie verhalten Sie sich verantwortungsbewusst? Glauben Sie nicht alles, was im Internet steht und surfen Sie stets mit einer gesunden Portion Misstrauen. Schützen Sie Ihren Computer und Ihre mobilen Geräte ausserdem mit einem sicheren Passwort.

Sehr oft ist die Benutzerin oder der Benutzer selbst das grösste Risiko – lassen Sie Ihren gesunden Menschenverstand walten. Beispielsweise beim Phishing geben sich Betrüger in E-Mails oder am Telefon z. B. als Ihr Finanzinstitut aus und versuchen Sie mit einem Link auf eine Website zu locken, die fast wie jene Ihres Finanzinstituts aussieht. Fallen Sie darauf herein und geben Ihre Zugangsdaten ein, können die Betrüger Ihr Konto plündern. **Denken Sie daran: Ein seriöses Finanzinstitut wird Sie niemals per E-Mail nach Ihren E-Banking-Zugangsdaten fragen.** Seien Sie also in einem gesunden Mass misstrauisch.

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.

Sorgfältiger Umgang mit Passwörtern

Kurze, nicht komplexe Passwörter sind unsicher, da sie von einem Angreifer herausgefunden werden können. Insbesondere Nachnamen, Namen von Kindern oder Haustieren, Wörter einer bekannten Sprache, Tastaturfolgen (z. B. «asdfg» oder «45678») sowie Geburtsdaten sollten nicht verwendet werden. **Am besten eignen sich willkürliche, mindestens 10-stellige Kombinationen aus Gross- und Kleinbuchstaben sowie Zahlen 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!**

- Wählen Sie lange Passwörter mit mindestens 10 Zeichen, bestehend aus willkürlichen Gross- und Kleinbuchstaben sowie Zahlen und Sonderzeichen.
- Teilen Sie Ihre Passwörter niemandem mit und bewahren Sie diese immer an einem sicheren Ort, wenn möglich verschlüsselt, auf.
- Speichern Sie in Ihrem Browser keine Passwörter für den Zugriff auf geschützte Webseiten ab. Browser verwalten diese Passwörter in der Regel nicht genügend sicher.

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

www.ebas.ch/step5

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

Lucerne University of
Applied Sciences and Arts

eBanking aber sicher!

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

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.ebankingabersicher.ch finden Interessierte praxisnahe Informationen zu notwendigen Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen.

- Hauptseite:
  https://www.ebankingabersicher.ch
  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

SKPPSC

Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
3001 Bern

www.skppsc.ch