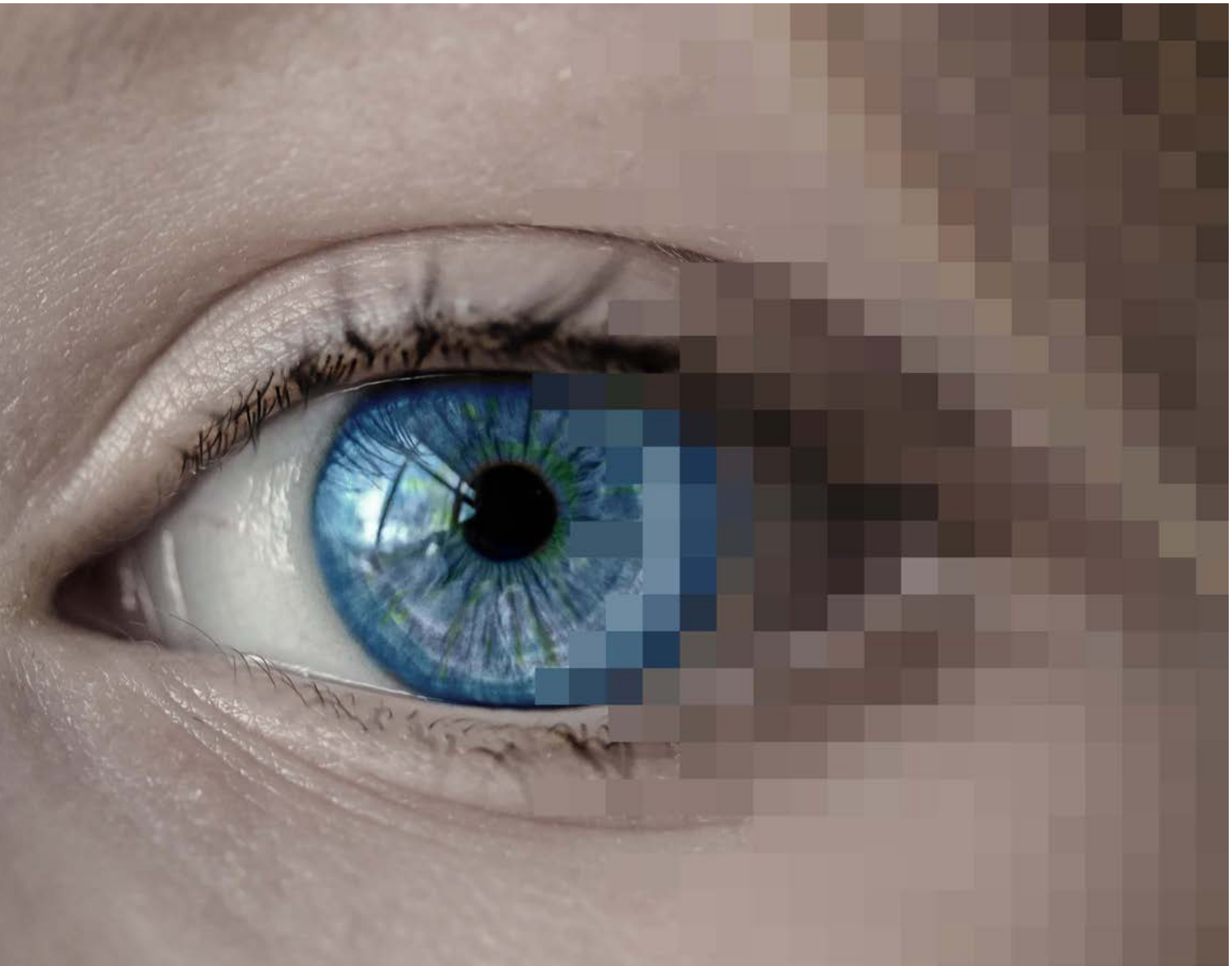
POLICE

Vier Säulen der Cybersicherheit
Informationen für Privatpersonen



Um sich gegen Cyberangriffe zu schützen, braucht es eine Kombination aus technischen Massnahmen und richtigem Verhalten. Die folgenden vier grundlegenden Präventionstipps helfen Ihnen, Ihre Sicherheit im Internet zu erhöhen und Angriffe zu bewältigen.

1 Bleiben Sie informiert

Lernen Sie die aktuellen kriminellen Handlungen im Internet und entsprechende Schutzmassnahmen kennen. Mit folgenden Websites bleiben Sie informiert:

> Kantonspolizei Bern, www.police.be.ch/cyber
> Nationales Zentrum für Cybersicherheit, www.ncsc.admin.ch
> Cybercrimepolice, www.cybercrimepolice.ch
> iBarry, www.ibarry.ch
> Schweizerische Kriminalprävention (SKP), www.skppsc.ch

2 Lassen Sie sich nicht hinters Licht führen

Schützen Sie Ihre Zugangsdaten
Geben Sie nie vertrauliche Informationen und Daten, z.B. Passwörter oder Kreditkarteninformationen, über unpersönliche Kanäle preis. Dies gilt auch für Formulare, welche Sie über einen Link in einem E-Mail, einem SMS oder auf einem Social-Media-Kanal geöffnet haben. Seriöse Dienstleister werden Sie nie über E-Mail, Kurznachricht oder Telefon zur Angabe von Passwörtern oder Kreditkartendaten auffordern.

Sich nicht unter Druck setzen lassen
Kriminelle nutzen Emotionen wie Angst, Neugier oder Vertrauen aus, um beispielsweise persönliche Informationen zu erschleichen oder Sie zu einer Überweisung zu bewegen. In vielen Fällen wird dabei Zeitdruck aufgebaut. Gehen Sie nicht auf Geld- und Wertsachenforderungen ein. Beenden Sie im Zweifelsfall das Telefonat oder löschen Sie unerwünschte Nachrichten. Melden Sie verdächtige Kontaktaufnahmen der Polizei.

Verweigern Sie den Zugriff
Kriminelle können sich beispielsweise als Mitarbeitende eines IT-Unternehmens, als Bankangestellte oder als Polizist/-in ausgeben. Gewähren Sie nie jemandem Zugang oder Fernzugriff zu Ihrem E-Banking, zu vertraulichen Daten oder zu Ihrem Computer.

Seien Sie misstrauisch
Seien Sie skeptisch gegenüber lukrativen Renditeangeboten, beträchtlichen Gewinnaussichten oder verlockenden Schnäppchen. Versprechen von grossen und einfachen Gewinnen in kurzer Zeit oder von überaus günstigen Angeboten sind typischerweise «zu gut, um wahr zu sein». Vorsicht ist ebenfalls gefragt, wenn jemand schnell von «grosser Liebe» spricht und später um finanzielle Unterstützung bittet.

Seien Sie auch sparsam mit dem Publizieren Ihrer persönlichen Informationen im Internet (z.B. Soziale Medien). Kriminelle sammeln diese, um ihre Attacken vorzubereiten.

3 Schützen Sie Ihre Systeme und Daten

Verwenden Sie sichere Passwörter
Ein Passwort sollte aus mindestens zwölf Zeichen, Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Idealerweise kommt es in keinem Wörterbuch vor, ist zufällig generiert und enthält keine persönlichen Informationen wie z.B. Ihr Geburtsdatum. Zusätzlichen Schutz bietet eine Zwei-Faktor-Authentifizierung. Wichtig: Generieren Sie für jede Anwendung ein eigenes Passwort. Ein Passwortmanager hilft Ihnen, die Passwörter zu verwalten.

Achten Sie auf ein geschütztes Netzwerk und aktualisierte Geräte
Viele neue Betriebssysteme haben bereits eine integrierte Firewall, einen Virenschutz und eine automatische Updatefunktion. Aktivieren Sie die entsprechenden Funktionen für sämtliche Geräte in Ihrem Netzwerk.

Die Modems der Internetprovider haben in vielen Fällen ebenfalls bereits einige Sicherheitsfunktionen integriert. Nutzen Sie diese und fragen Sie im Zweifelsfall bei Ihrem Provider nach.

Die Sicherheit kann zusätzlich erhöht werden, wenn zwischen Modem und Heimnetzwerk weitere Sicherheitskomponenten, wie beispielsweise Router mit Angriffserkennungs- und Angriffsschutz-System (IDS und IPS) oder Webfiltern (DNS-Filter), eingebaut werden. Diverse Router können ausserdem verschiedene Netzwerksegmente wie Gast- und Heimnetzwerk verwalten. Damit ermöglichen Sie Besuchern oder auch smarten Haushaltsgeräten Internetzugang, ohne Ihr Hauptnetz zu gefährden. Nutzen Sie diese Einstellungen.

All-in-one-Lösungen bieten sogenannte Unified-Threat-Management-Systeme. Diese umfassende Sicherheitslösung gibt es als Hardware-, Software- oder Cloudlösung.

Sichern Sie Ihre Daten
Diverse Betriebssysteme bieten bereits integrierte Back-up-Lösungen. Diese Lösungen sind handlich und sichern die Daten kontinuierlich. Weil Nutzerinnen und Nutzer sie jedoch oft mit dem Computer verbunden lassen, sind sie anfällig für Verschlüsselungsangriffe. Lagern Sie deshalb zusätzlich eine Kopie Ihres Back-ups getrennt (offline) und eine weitere in einer Cloud (ausser Haus). Prüfen Sie in regelmässigen Abständen, ob Ihre Daten tatsächlich in den Back-ups enthalten sind und wiederhergestellt werden können.

4 Was Sie im Schadensfall tun können

Erste Hilfe bei einem Cyberangriff
Trennen Sie alle Systeme umgehend vom Netzwerk/Internet. Vergessen Sie nicht, das WLAN auszuschalten. Wählen Sie die Notrufnummer 112 oder kontaktieren Sie eine Polizeiwache in Ihrer Nähe (www.suisse-epolice.ch). Warten Sie mit dem Wiederaufsetzen der Systeme, bis die Polizei die Spuren gesichert hat.

Jede Meldung zählt
Melden Sie strafrechtlich relevante Vorfälle, beispielsweise Hacking, Diebstahl oder Erpressung, möglichst schnell der Polizei. Besonders dann, wenn ein Schaden entstanden ist.

Falls kein Schaden entstanden ist, können Sie den Vorfall auch beim Nationalen Zentrum für Cybersicherheit melden (www.ncsc.admin.ch).

Jede Anzeige und jede Meldung kann den entscheidenden Hinweis zu einer Täterschaft liefern.

Suchen Sie Hilfe
Die Folgen einer kriminellen Tat können eine finanzielle und/oder psychische Belastung sein. Scheuen Sie sich nicht, professionelle Hilfe zur Bewältigung des Erlebten zu suchen. Ein erster Schritt kann ein Anruf bei einer Hilfsorganisation sein. Auf der Website der Opferhilfe Schweiz (www.opferhilfe-schweiz.ch) finden Sie beispielsweise diverse Beratungsstellen im Kanton Bern.

Kantonspolizei Bern
Waisenhausplatz 32
3011 Bern

police.be.ch