# Schutzmassnahmen gegen Cyberkriminalität

Die Bedrohungen aus dem Internet werden immer ausgefeilter. Spezifisch das Gesundheitswesen mit seinen schützenswerten Daten wird verstärkt Ziel von Erpressungen oder schädlichen Inhalten. In diesem Factsheet sind deshalb die wichtigsten Schutzmassnahmen und Verhaltensregeln gegen Cyberkriminalität aufgelistet – um sensible Gesundheitsdaten noch besser zu schützen.

## Technische Massnahmen

- Systeme immer auf dem neusten Stand halten (Browser, Virenschutzprogramm, Betriebssystem etc.) und **Updates umgehend installieren.**
- **Firewall und Virenscanner** sind ein Muss – auch auf Apple Geräten.
- Regelmässige **Backups** mit einer sicheren Aufbewahrung. Auch Restore prüfen!
- **Limitierende Benutzerberechtigungen** setzen und nicht mit dem Administrator-Account arbeiten.
- **Alle Geräte,** die direkt am Internet angeschlossen sind (Webcam, Router, Handy…), gehören geschützt durch sichere Passwörter und konsequente Updates.
- Option **«Dateierweiterungen anzeigen»** in den Windows-Einstellungen aktivieren, um potenziell schädliche Dateien zu erkennen. In Anhängen nicht auf Dateierweiterungen wie ‹.exe›, ‹.vbs›, ‹.bat›, ‹.com› und ‹.scr› klicken.

## Verhaltensregeln

- Ein **sicheres Passwort** ist extrem wichtig. Acht bis zehn Stellen inklusive Zahlen und Sonderzeichen sind das Minimum. **Merkhilfen** verwenden!
- **Vorsicht bei nicht bekannten Absendern.** Öffnen Sie Anhänge in E-Mails von jemandem den Sie nicht kennen nur mit Vorsicht.
- Schädlinge verbreiten sich meist via E-Mail, deshalb ist ein sorgsamer Umgang zwingend: **Anhänge nie direkt öffnen** und Vorsicht beim Adressen publizieren.
- Vorsicht beim Surfen! **Keine unbekannten Programme herunterladen.** Bei der Angabe von Informationen auf Verschlüsselung achten (Schloss-Symbol) und Serveradressen genau prüfen – im Zweifel den Anbieter anrufen.
- Sensible Daten nur **verschlüsselt** an sicher identifizierte Empfänger übermitteln.

## Organisatorische Massnahmen

- **Informationssicherheit ist Chef-Sache** und bedingt Vorgaben, Weisungen (z.B. Herausgabe von Daten) und Prozesse (z.B. Backup).
- Die **Awareness der Mitarbeiter** hat höchste Priorität, deshalb sind regelmässige Schulungen und aktuelle Informationen notwendig.