LUZERNERPOLIZEI

Hacking und Malware

Mit der Einhaltung bestimmter Verhaltensregeln in Kombination mit technischen Vorkehrungen können die eigenen Daten vor Malware- und Hacking-Angriffen geschützt werden.

Hacking

- Unter Hacking versteht man das Eindringen in ein fremdes Computersystem durch Hacker. In den meisten Fällen nutzen Hacker unbemerkte Sicherheitslücken.
- Sobald der Zugang zum Computersystem gefunden wurde und unbemerkt bleibt, können Hacker Inhalte und Strukturen des Systems nach Belieben verändern.
- Die Motive der Hacker sowie die Konsequenzen eines solchen Angriffs können stark variieren.

Malware

- Malware (Schadsoftware) kommt zum Einsatz, wenn Hacker den Zugang zu einer Webseite, einem E-Mail-Konto oder Computer offen gelegt haben und schädliche Aktionen auf den fremden Computersystemen ausgeführt werden.
- Ein zusätzliches Einfallstor für Malware sind schädliche Dateien, welche in E-Mails verschickt oder auf Webseiten platziert werden.

So schützen Sie sich

Technische Massnahmen

- Aktivieren Sie die automatische Update-Funktion für Ihr Betriebssystem, Ihre Programme und Apps.
- 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.
- Sichern Sie Ihre Daten regelmässig auf einer externen Festplatte, DVD, CD oder online in einem Cloud-Speicher.

Passwort

- Schützen Sie Ihren Computer und mobilen Geräte (Smartphones, Tablets etc.) vor unbefugtem Zugriff und sperren Sie den Bildschirm, wenn Sie nicht aktiv am Gerät arbeiten.
- Wählen Sie ein starkes Passwort. Das Passwort sollte mindestens 12 Zeichen beinhalten und aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen bestehen.
- Benutzen Sie für jeden Dienst ein anderes Passwort.
- Nutzen Sie wenn möglich die Zwei-Faktor-Authentifizierung.
- Nutzen Sie einen Passwort-Manager.

E-Mail

- Misstrauen Sie E-Mails mit unbekannter Absenderadresse.
- Klicken Sie in verdächtigen E-Mails auf keine Anhänge und folgen Sie keinen Links (Phishing).
- Öffnen Sie nur Dateien oder Programme aus vertrauenswürdigen Quellen und nur nach vorgängiger Prüfung mit einer aktuellen Antiviren-Software.
- Antworten Sie nicht auf Spam, sonst wird die E-Mail-Adresse gültig erkannt und es wird weiter Spam geschickt.

Surfen im Internet

- 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.

Die Luzerner Polizei beantwortet gerne Ihre Fragen.

117 POLIZEI-NOTRUF

Luzerner Polizei | Prävention | Centralstrasse 21 | 6210 Sursee | Tel 041 289 24 44 | praevention.polizei@lu.ch | www.polizei.lu.ch

Version 01/2024