LUZERNERPOLIZEI

Phishing

Bei Phishing handelt es sich um eine Form von Online-Betrug. Durch gefälschte Kommunikation versucht die Täterschaft, persönliche Informationen wie Passwörter, Kreditkartendaten oder andere sensible Daten von Nutzern zu stehlen. Dabei nutzt die Täterschaft Social Engineering, wobei die Gutgläubigkeit des Opfers ausgenutzt wird. Phishing-Nachrichten werden meist per E-Mail oder Instant Messaging versandt, mit dem Ziel Vermögensdelikte zu begehen.

Vorgehen der Täterschaft

- Massenversand von E-Mails mit gefälschtem oder nachgeahmtem Absender, z.B. einer Bank.
- E-Mails enthalten meist einen Link zu einer nachgeahmten Webseite.
- Formulare fordern zur Eingabe von persönlichen Daten, z.B. zu Sicherheitszwecken oder für Rückerstattungen, auf.
- Die Absenderadresse von Phishing-Mails, deren Inhalt sowie die Gestaltung der Webseite, auf welche sie verweisen, ahmen nahezu identisch Finanzinstitute, Behörden oder Ämter nach.
- Es kommt vor, dass legitime Webseiten gehackt werden, um Phishing-Seiten einzufügen.
- Die Täter versenden die E-Mails manchmal gezielt («Spear Phishing») und nicht in Massenmails.
- Nebst den Bankdaten verlangt die Täterschaft auch andere persönliche Daten, wie Name, Vorname, Benutzername und Passwörter für jegliche Konten.

So schützen Sie sich

- Seien Sie misstrauisch bei E-Mails mit einer allgemeinen Anrede und die «umgehendes Handeln» erfordern.
- Ein Link in einer E-Mail? Fahren Sie mit der Maus darüber und finden Sie heraus, wo der Link wirklich hinführt.
- Beantworten Sie niemals E-Mail-Anfragen nach Passwörtern, Sicherheitscodes oder andere sensitiven Daten.
- Öffnen Sie nur E-Mail-Anhänge von Absendern, denen Sie vertrauen.
- Seien Sie misstrauisch gegenüber E-Mails mit Rechtschreib- und Grammatikfehlern.
- Behandeln Sie E-Mails von einem bekannten Absender, aber ungewöhnlicher E-Mail-Adresse mit Vorsicht.
- Melden Sie verdächtige E-Mails an das Nationale Zentrum für Cybersicherheit:
  https://www.antiphishing.ch/de/

Wenn es trotzdem passiert

- Nehmen Sie Kontakt zu Ihrer Bank auf und sperren Sie Ihre Kreditkarte und gegebenenfalls Ihr Konto.
- Informieren Sie Unternehmen oder Institutionen, von denen die E-Mail vermeintlich versendet wurde.
- Ändern Sie alle Passwörter, die gestohlen worden sein könnten.
- Beobachten Sie all Ihre Online-Konten und melden Sie verdächtige Vorfälle.
- Stellen Sie sicher, dass Ihr Antivirenprogramm auf dem neusten Stand ist und starten Sie einen Virenscan auf Ihrem Computer.
- Melden Sie sich bei der Polizei und stellen Sie Anzeige.

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