Liesing, im September 2023

Geschätzte Lesachtalerinnen und Lesachtaler,

liebe Jugend!

GEMEINSAM.

SICHER mit ihrer Polizei

Phishing-Mails:

Woran Sie sie erkennen und worauf Sie achten müssen

Phishing ist der Versand gefälschter E-Mails, die Menschen dazu verleiten sollen, auf einen Betrug hereinzufallen. Phishing-Mails zielen häufig darauf ab, dass die Nutzer Finanzinformationen, Zugangsdaten oder andere sensible Daten preisgeben.

Die Ziele der Angreifer variieren, aber meist geht es darum, persönliche Informationen oder Zugangsdaten zu stehlen. Dabei vermittelt die Phishing-E-Mail ein Gefühl der Dringlichkeit, indem sie der Zielperson die Sperrung ihres Accounts oder finanzielle Verluste androht. Durch die Dringlichkeit nehmen sich die Nutzer nicht mehr die Zeit, über die Forderungen der Angreifer nachzudenken, sondern gehen darauf ein. Erst später erkennen Sie Warnzeichen und sehen, dass die Forderungen eigentlich unangemessen waren.

Wenn man zu Hause oder am Arbeitsplatz auf eine Phishing-Attacke hereinfällt, ist es wichtig, sich die Folgen bewusst zu machen. Im Folgenden sind einige der Probleme aufgeführt, die auftreten können:

- Geld wird aus Bankkonten gestohlen.
- Kreditkarten werden von Betrügern belastet.
- Steuererklärungen werden im Namen der betrogenen Person eingereicht.
- Auf den Namen der betrogenen Person werden Darlehen und Hypotheken eröffnet.
- Verlorener Zugang zu Fotos, Videos, Dateien und anderen wichtigen Dokumenten.
- Gefälschte Social-Media-Beiträge in den Konten der betrogenen Person.
- Online-Überweisungen an das Konto des Angreifers.
- Ransomware, die Geld von Opfern erpresst.
- Dateien werden gesperrt und unzugänglich.

Wenn Sie nicht eindeutig entscheiden können, ob eine E-Mail echt ist und Sie einen Betrugsversuch vermuten, fragen Sie beim echten Anbieter nach.
Aber auch hier gilt: Klicken Sie nicht auf Links, öffnen Sie keinen Dateianhang, antworten Sie nicht auf diese E-Mail. Sie sollten auch keine Kontaktmöglichkeit nutzen, die in der E-Mail angegeben ist. Suchen Sie besser eine Filiale des echten Anbieters auf oder nutzen Sie eine Kontaktmöglichkeit auf der echten Internetseite des Anbieters.

Wie schützt man sich gegen Phishing?

Keine sensiblen Daten per E-Mail herausgeben

Grundregel: Kein Kreditkarteninstitut und kein seriöser Anbieter fordert Sie per E-Mail auf, vertrauliche Zugangsdaten preiszugeben – auch nicht um der Sicherheit willen.

Was Sie außerdem beachten sollten, wenn Sie Daten- oder Passwortdiebstahl entgehen möchten:

- Überprüfen Sie stets die **Adressleiste in Ihrem Browser**. Am besten tragen Sie die Adressen zu häufig besuchten Login-Seiten in die Favoritenliste Ihres Browsers ein.
- Klicken Sie niemals auf **Links in einer dubiosen E-Mail**. Versuchen Sie im Zweifelsfall stattdessen, die im E-Mail-Text genannte Seite über die Startseite der betreffenden Organisation zu erreichen – also ohne den angegebenen Link in die Adresszeile des Browsers einzutippen.
- Wenn Sie sich nicht sicher sind, ob eine E-Mail vielleicht berechtigter Weise nach vertraulichen Daten fragt, **fragen Sie am besten telefonisch** bei dem genannten Anbieter nach.
- Geben Sie **keinesfalls persönliche Daten wie Passwörter, Kreditkarten- oder Transaktionsnummern via E-Mail** preis – egal, wie vertrauenserweckend die betreffende E-Mail erscheint.
- Geben Sie persönliche Informationen nur in der gewohnten Weise etwa auf der Online-Banking-Website ein. **Sobald Ihnen irgendetwas seltsam vorkommt**, beenden Sie die Verbindung sofort und kontaktieren Sie den regulären Website-Betreiber.
- **Starten Sie niemals einen Download-Link direkt aus einer E-Mail** heraus, auf deren Echtheit Sie sich nicht hundertprozentig verlassen können. Starten Sie, wenn möglich, einen Download stets direkt von der Anbieter-Website.
- Öffnen Sie insbesondere niemals Dateien im **Anhang einer verdächtigen E-Mail**.
- Beenden Sie jede **Online-Session durch einen regulären Log-out** – statt einfach nur das Browserfenster zu schließen.
- Kontrollieren Sie regelmäßig den **Saldo Ihres Bankkontos sowie Umsätze** zum Beispiel von Internetzahlungsdienstleistern. So können Sie bei unbefugten Abbuchungen schneller reagieren.

- Geben Sie niemals persönliche Daten auf Webseiten mit unverschlüsselter Verbindung ein. Ob eine Website verschlüsselt mit Ihrem Browser kommuniziert, erkennen Sie an der Abkürzung **"https://"** in der Adresszeile sowie an dem kleinen Vorhängeschloss- Symbol neben der Adresszeile des Browsers.
- Achten Sie stets darauf, dass Ihre **Antivirus-Software aktuell und die Firewall aktiv** ist.

Gerne verweisen wir an dieser Stelle auch auf die Möglichkeit einer **kostenlosen, (kriminal-) polizeilichen Beratung:**

Kontakt: Polizeiinspektion Liesing, Tel 059133/ 2213 oder

pi-k-liesing@polizei.gv.at

Mit freundlichen Grüßen,

die Bediensteten der Polizeiinspektion Liesing