Phishing/Smishing

Phishing bedeutet Datendiebstahl. Beim Phishing versuchen Angreiferinnen und Angreifer, Sie dazu zu bringen, vertrauliche Informationen wie Passwörter oder Bankdaten preiszugeben. In E-Mails, SMS oder Websites tarnen sie sich als vertrauenswürdige Personen oder Institutionen, um an Ihre Daten zu gelangen. Das Ziel dabei ist, Zugriff auf Ihre Konten oder Ihr Computersystem zu erhalten, um Ihr Geld zu stehlen oder Ihre Identität anzunehmen.

Sollte der Phishing-Angriff über eine SMS oder einen Messenger-Dienst erfolgen, spricht man von Smishing.

Typische Warnsignale

- Der Text der Nachricht weist auf einen dringenden Handlungsbedarf hin.
- Der dringende Handlungsbedarf ist mit angedrohten Konsequenzen verbunden.
- Sie werden aufgefordert, vertrauliche Informationen bekannt zu geben oder einem Link zu folgen.
- Obwohl Personen, Firma oder Behörde Ihnen bekannt erscheinen, ist die Aufforderung der Absenderin bzw. des Absenders ungewöhnlich.
- Die Anrede in der Nachricht ist unpersönlich („Sehr geehrte Kundin / Sehr geehrter Kunde“ oder „Nutzerin/Nutzer“).

Präventionsempfehlungen der Polizei

- ✓ Prüfen Sie die Absenderin bzw. den Absender von Nachrichten. Weist sie bzw. er seltsame Schreibweisen, Zahlen oder Ergänzungen auf?
- ✓ Prüfen Sie jeden Link sorgfältig, bevor Sie ihm folgen. Meist ist es besser, die Seiten direkt aufzurufen, anstatt einem Link zu folgen.
- ✓ Verwenden Sie Zwei-Faktor-Authentifizierung.
- ✗ Seien Sie bei Nachrichten von unbekannten Absenderinnen bzw. Absendern skeptisch.
- ✗ Bankmitarbeitende fragen Sie nie nach persönlichen Daten oder TAN.
- ✗ Lassen Sie sich nicht durch angedrohte Konsequenzen unter Druck setzen.

Maßnahmen im Schadensfall

- Ändern Sie ihre Zugangsdaten und Passwörter.
- Lassen Sie unverzüglich Ihre Online-Banking-Dienste bzw. Ihr Bankkonto und Ihre Bankkarten sperren.
- Sollte ein Schaden entstanden sein, erstatten Sie Anzeige bei der Polizei.
- Überwachen Sie Ihre Kontobewegungen und dokumentieren Sie die Zahlungs- und Kontoinformationen der Betrügerinnen und Betrüger.
- Bei Betrugsverdacht können Sie sich an die **Cybercrime-Meldestelle** des Bundeskriminalamtes unter against-cybercrime@bmi.gv.at wenden (diese Meldung ersetzt nicht die Anzeige).
- Wenn Ihr Unternehmen von einem Cyberangriff, Ransomware oder Verschlüsselungstrojanern betroffen ist, können Sie sich an die **Cybersecurity-Hotline** der Wirtschaftskammer Österreich unter 0800 888 133 wenden.

Weiterführende Links

- Polizeiliche Kriminalprävention www.kriminalpraevention.gv.at
- Watchlist Internet – Online-Betrug, -Fallen & -Fakes im Blick
- Internet Ombudsstelle | Kostenlose Streitschlichtung & Beratung in Österreich
- Home - Saferinternet.at
- Internet-Falle melden