Smishing, Vishing, Phishing – oder was?

Frankfurt, 7. Juni 2023 – Der Begriff „Phishing" ist vielen Menschen inzwischen bekannt. Doch was verbirgt sich hinter „Smishing" und „Vishing"? Alle drei Social-Engineering-Attacken haben das gleiche Ziel: Durch gezielte Täuschung und Irreführung von Kundinnen und Kunden an sensible Informationen wie Online-Banking-Zugänge, PINs, TANs, Konto- oder Kreditkartenummern zu kommen. Werden Daten herausgegeben, nehmen die Täter:innen unberechtigte und damit kriminelle Transaktionen zu Lasten der Verbraucher:innen vor.

Das Internetportal kartensicherheit.de klärt über die Unterschiede der Methoden auf:

Gefährliche E-Mails: Phishing

Phishing setzt sich zusammen aus „Passwort" und „Fishing". Kriminelle versuchen mittels gefälschter E-Mails persönliche Zugangsdaten abzugreifen. Sie täuschen dringenden Handlungsbedarf vor, da sonst beispielsweise die Sperrung des Kontos drohen würde. Mit dem Klick auf einen Weblink und Eingabe der Login-Daten landen diese in den Händen der Cyber-Kriminellen. Oftmals beinhalten die E-Mails auch schädliche Anhänge, die weiteren Zugang zu wertvollen Daten liefern.

Betrug per SMS oder WhatsApp: Smishing

Bei dieser Kombination aus „SMS" und „Phishing" fordert eine Textnachricht am Handy dazu auf, einem Link zu folgen oder eine Telefonnummer anzurufen. Dabei sollen angeblich das Konto geprüft oder Daten aktualisiert werden. Der Link führt allerdings zu einer gefälschten Webseite oder der Anruf zu einem angeblichen Mitarbeitenden eines real existierenden Unternehmens.

Unerwünschte Anrufe: Vishing

Beim „Voice-Phishing" läuft der Kontakt übers Telefon. Die Anrufer:innen wirken sehr vertrauenswürdig und geben vor, vermeintliche Sicherheitsprobleme lösen zu müssen. Die Kriminellen verleiten dazu, geheime Daten herauszugeben oder direkt Geld zu überweisen. Auf mögliche Einwände und Zweifel reagieren sie mit glaubwürdigen Argumenten.

Wie kann man sich schützen?

- Banken und Sparkassen, Behörden oder seriöse Firmen fragen Sie niemals nach vertraulichen Informationen – weder telefonisch noch digital!

- Folgen Sie keinen Links, bei denen zur Eingabe von PINs, TANs, Passwörtern, Konto- oder Kreditkartennummern aufgefordert wird.
- Reagieren Sie nicht auf unübliche E-Mails, SMS oder Anrufe. Anhänge, Links und Bilder sollten Sie nicht öffnen, ohne vorher genau zu prüfen, von wem sie stammen.
- Lassen Sie sich nicht unter Druck setzen! Fragen Sie im Zweifel lieber direkt bei Ihrer persönlichen Kundenberatung der Bank oder Sparkasse nach. Das hat auch Zeit, bis das Institut wieder geöffnet ist.
- Sollten Sie trotz aller Vorsicht auf Kriminelle hereingefallen sein und vertrauliche Daten weitergegeben haben, sperren Sie sofort das Online-Banking. Entweder direkt bei Ihrem Kreditinstitut oder beim Sperr-Notruf 116 116*.

* Der Service des Sperr-Notrufs ist kostenlos. Auch der Anruf bei der 116 116 aus dem deutschen Festnetz ist gebührenfrei. Aus dem Mobilnetz und aus dem Ausland können Gebühren anfallen. Sollte der Sperr- Notruf in seltenen Fällen aus dem Ausland nicht erreicht werden können, gibt es alternativ die Rufnummer +49 (0) 30 4050 4050.

Weitere Tipps zum richtigen Umgang mit Karte und PIN hat die EURO Kartensysteme GmbH in Zusammenarbeit mit der Deutschen Kreditwirtschaft im Internetportal www.kartensicherheit.de zusammengestellt. Hier finden Verbraucher:innen viele interessante Informationen zu bargeldlosen Zahlungsmitteln.

Pressemeldung abrufbar unter www.kartensicherheit.de

Übermittelt durch:
Schwarz & Sprenger GmbH – Telefon: +49 (0) 89 / 2153 7887 0 – www.schwarz-sprenger.de