PHISHING: CHECKLISTE FÜR DEN ERNSTFALL

WAS IST PHISHING?

Cyber-Kriminelle verschicken betrügerische Nachrichten per E-Mail, über Messenger oder über soziale Netzwerke. Sie fordern Nutzerinnen und Nutzer dazu auf, vertrauliche Informationen wie Passwörter, Zugangsdaten oder Kreditkartennummern preiszugeben. Angeschriebene sollen auf einen Link klicken.

Die Gefahr: Die angegebenen Links führen auf gefälschte Internetseiten, auf denen die Daten abgegriffen werden. Die Nachrichten wirken täuschend echt, die Absender seriös. Viele Empfänger schöpfen daher keinen Verdacht und geben ihre Daten den Kriminellen preis.

DAS SOLLTEN SIE TUN, WENN …

… Sie Zahlungsdaten weitergegeben haben:

- ✓ Sperren Sie Ihr Bankkonto.
- ✓ Kontrollieren Sie die Umsätze Ihres Bankkontos und setzen Sie sich mit Ihrer Bank in Verbindung.
- ✓ Nutzen Sie nach der Entsperrung ausschließlich neue Passwörter und PINs für Ihr Konto.

… Sie Zugangsdaten zu Ihrem E-Mail-Konto weitergegeben haben:

- ✓ Vergeben Sie ein neues Passwort.
- ✓ Es kann sein, dass mit dem Zugang zu Ihrem E-Mail-Postfach auch die Zugänge anderer Online-Dienste kompromittiert sind und beispielsweise geändert oder übernommen wurden. Deswegen müssen Sie diese ebenfalls zurücksetzen. Das gilt für Online-Profile, mit denen Sie sich bei anderen Diensten, z. B. einem Online-Shop, anmelden können.

… Sie Zugangsdaten zu anderen Konten, z. B. Online-Shops, weitergegeben haben:

- ✓ Vergeben Sie ein neues Passwort.
- ✓ Nehmen Sie Kontakt mit dem Anbieter auf.
- ✓ Überprüfen Sie zudem, ob Zahlungsdaten betroffen waren und nehmen Sie dementsprechend auch Kontakt mit Ihrer Bank auf.

HINWEIS

Vergeben Sie für alle Online-Account-Zugänge jeweils unterschiedliche Passwörter. Passwort-Manager können dabei hilfreich sein.

Bundesamt
für Sicherheit in der
Informationstechnik

DAS SOLLTEN SIE TUN, WENN …

… Sie auf einen Link geklickt haben und Geldforderungen bekommen:

- ✓ Zahlen Sie kein Geld an Kriminelle.
- ✓ Wenden Sie sich bei Geldforderungen Unbekannter an die Polizei, die Verbraucherzentrale oder suchen Sie Rat bei einem Rechtsbeistand.

… den Verdacht haben, dass Ihre Daten abgeschöpft wurden:

- ✓ Erstatten Sie in jedem Fall Anzeige bei Ihrer örtlichen Polizeidienststelle – auch bei einem vagen Verdacht. Als Opfer von Internetkriminalität haben Sie die gleichen Rechte wie Opfer anderer Straftaten auch.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR PHISHING

- › Führen Sie Aktualisierungen von Software und Betriebssystemen auf allen Geräten immer sofort durch und installieren Sie Antivirenprogramme.
- › Seien Sie skeptisch bei E-Mails unbekannter Absender. Ihre Bank, Diensteanbieter oder Behörden bitten niemals per E-Mail darum, persönliche Daten wie Passwörter über einen Link zu ändern.
- › Bei Zweifeln lassen Sie sich die Echtheit einer E-Mail vom Absender telefonisch bestätigen. Nutzen Sie dafür nicht die Telefonnummer aus der E-Mail, sondern suchen Sie diese selbst heraus.
- › Vorsicht bei Anhängen mit Formaten wie **.exe** oder **.scr**. Diese können Schadsoftware direkt auf Ihr Gerät laden. Manchmal werden Nutzer oder Nutzerinnen auch durch Doppelendungen wie Dokument **.pdf.exe** in die Irre geführt.
- › Verwenden Sie für die diversen Account-Zugänge möglichst eine Zwei-Faktor-Authentisierung. Durch die zweite Stufe der Identifizierung können Kriminelle selbst dann nicht auf Ihre Daten zugreifen, wenn sie bereits Ihr Passwort erbeutet haben.

Mehr Informationen zum Schutz vor Betrüger-E-Mails unter:
www.bsi-fuer-buerger.de/phishing

Mehr Informationen für Opfer von Internetkriminalität:
www.polizei-beratung.de/opferinformationen/cybercrime/

Bundesamt
für Sicherheit in der
Informationstechnik