PHISHING: CHECKLISTE FÜR DEN ERNSTFALL

WAS IST PHISHING?

Kriminelle versuchen, an vertrauliche Informationen wie Passwörter oder Kreditkartendaten zu gelangen. Dafür verschicken sie betrügerische Nachrichten – zum Beispiel per E-Mail, per SMS oder über Messengerdienste und soziale Netzwerke. Angeschriebene fordern sie unter einem Vorwand auf, einen Link zu öffnen.

In vielen Fällen führen solche Links jedoch zu gefälschten Internetseiten. Diese ähneln etwa denen von Banken oder Onlineshops stark. Dort sollen Angeschriebene anschließend ihre Daten eingeben. Die Kriminellen greifen dann etwa Passwörter ab. Oft wirken die Internetseiten dabei täuschend echt und die Absenderinnen und Absender seriös.

DAS SOLLTEN SIE TUN, WENN...

... Sie Zahlungsdaten, beispielsweise Ihre Kreditkarteninformationen oder die Login-Daten für Ihr Onlinebanking-Konto, an Unbefugte weitergegeben haben:

- ✓ **Kontrollieren Sie die Umsätze Ihres Bankkontos den kostenfreien Sperr-Notruf 116 116 oder aus dem Ausland über die gebührenpflichtige Sperr-Hotline +49 116 116.**
- ✓ **Kontrollieren Sie die Umsätze Ihres Bankkontos** und setzen Sie sich mit Ihrer Bank zu weiteren Schritten in Verbindung.
- ✓ **Nutzen Sie nach der Entsperrung ausschließlich neue Passwörter und PINs.**

... Sie Zugangsdaten zu einem Benutzerkonto, zum Beispiel Ihrem E-Mail-Konto oder Ihrem Account bei einem Onlineshop, weitergegeben haben:

- ✓ **Vergeben Sie schnellstmöglich ein neues Passwort.**
- ✓ **Beenden Sie unmittelbar danach in den Einstellungen alle aktiven Sitzungen.** Sollten Unbefugte auf anderen Geräten eingeloggt sein, verlieren sie nun Zugriff zu Ihrem Benutzerkonto.
- ✓ **Überprüfen Sie, ob zum Beispiel Einstellungen geändert oder Einkäufe getätigt wurden.** Falls Sie diese nicht rückgängig machen können, nehmen Sie Kontakt zum Anbieter, etwa dem E-Mail-Anbieter oder dem Shop-Betreiber, auf.
- ✓ **Kontaktieren Sie den Anbieter auch, wenn Sie nicht länger auf Ihr Benutzerkonto zugreifen können.** Möglicherweise haben Unbefugte das Passwort geändert.
- ✓ **Schauen Sie nach, ob Kontodaten in Ihrem Benutzerkonto einsehbar waren.** Falls Unbefugte diese womöglich auslesen konnten, informieren Sie Ihre Bank.
- ✓ **Überprüfen Sie, ob weitere Benutzerkonten kompromittiert sein könnten.** Das kann insbesondere bei gehackten E-Mail-Konten der Fall sein, wenn Sie die E-Mail-Adresse zum Zurücksetzen des Passworts hinterlegt haben oder sich per Single-Sign-On (Anmeldung über Drittanbieter) anmelden. Ändern Sie dann auch bei diesen Benutzerkonten das Passwort.

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei

HINWEIS

Schützen Sie Ihre Benutzerkonten entweder mit einem starken Passwort und der Zwei-Faktor-Authentisierung oder mithilfe von Passkeys als passwortlose Alternative.

… Sie Geldforderungen erhalten, nachdem Sie zum Beispiel auf einen Link in einer gefälschten E-Mail geklickt haben:

- ✓ **Zahlen Sie kein Geld an Kriminelle.** Nicht zuletzt ermutigen Sie Kriminelle sonst zu weiteren Forderungen und Angriffen.
- ✓ **Wenden Sie sich an die Polizei, die Verbraucherzentrale oder suchen Sie Rat bei einem Rechtsbeistand.**

HINWEIS

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

- Seien Sie skeptisch gegenüber **E-Mails unbekannter Absender.** Banken und Behörden bitten beispielsweise niemals per E-Mail um die Herausgabe eines Passworts. Sicherheitsbewusste Institutionen bitten auch nicht per E-Mail darum, sensible Daten über einen Link zu ändern. Mitunter fälschen Kriminelle außerdem die Absenderadresse.
- Lassen Sie sich die Echtheit einer E-Mail im Zweifelsfall **telefonisch bestätigen.** Nutzen Sie dafür nicht die Telefonnummer aus der E-Mail, sondern suchen Sie diese selbst heraus.
- Seien Sie **vorsichtig bei Anhängen,** insbesondere bei solchen mit Formaten wie .exe oder .scr. Diese können Schadsoftware direkt auf Ihr Gerät laden. Öffnen Sie solche Anhänge also nur, wenn Sie sicher sind, was sie im Einzelnen bewirken. Manchmal werden Nutzerinnen und Nutzer auch durch Doppelendungen wie .pdf.exe in die Irre geführt.
- Öffnen Sie nicht unüberlegt **QR-Codes.** Auch diese können als Links fungieren und führen möglicherweise zu gefälschten Internetseiten.
- Aktivieren Sie die **Zwei-Faktor-Authentisierung** für Ihre Benutzerkonten, wo möglich. So können Kriminelle selbst dann nicht auf diese zugreifen, wenn sie Ihre Passwörter erbeutet haben. Eine Alternative zu Passwörtern stellen zudem Passkeys dar.
- Bestätigen Sie den sogenannten **zweiten Faktor** nicht, wenn andere Sie darum bitten. Mitunter kontaktieren Kriminelle, die ein Passwort erlangt haben, ihre Opfer zum Beispiel telefonisch und fordern sie unter einem Vorwand dazu auf, den zweiten Faktor beispielsweise über eine dafür vorgesehene Smartphone-App zu bestätigen.
- Installieren Sie **Antivirenprogramme** oder aktivieren Sie vorinstallierte Antivirenfunktionen Ihres Betriebssystems. Führen Sie zudem Aktualisierungen Ihres Betriebssystems und Ihrer Anwendungen auf allen Geräten durch, sobald entsprechende Updates verfügbar sind.

Mehr Informationen rund um Cybersicherheit:
www.bsi.bund.de/VerbraucherInnen

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

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei