Der Begriff Phishing

Phishing (sprich: fisching) ist eine Art von Daten-Diebstahl, eine Betrugsvariante. Phishing ist ein zusammengesetztes Wort und kommt von „**P**assword“ und „**fishing**“. Dabei geht es um das Ausspionieren von persönlichen Daten wie etwa Kreditkartennummern und Kontodaten sowie Bankkonto-Zugangsdaten.

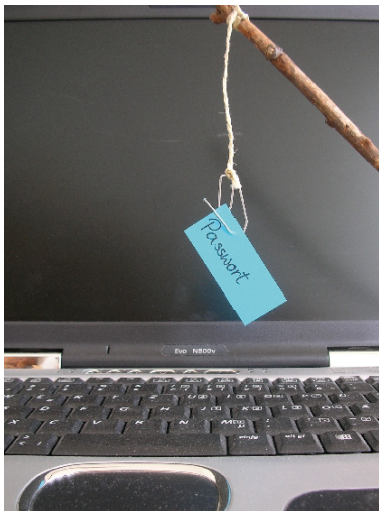

Bild: ifs Schuldenberatung

Was ist daran gefährlich?

Die Methode ist fast immer gleich. Die Täter:innen senden E-Mails, die einen falschen Link (Verweis) zu einer Website enthalten. In dem E-Mail steht geschrieben, dass man auf den Link klicken und dann seine Daten eingeben soll. Als Grund wird oft eine Sicherheitsüberprüfung angegeben.
Der Link sieht auf den ersten Blick aus, als führe er zur Website des echten Unternehmens. Der Schein trügt aber, denn wer auf den Link klickt, der gelangt zu der Website der Betrüger:innen. Da diese Seite fast so aussieht wie die Seite der richtigen Firma, geben Leute ihre Daten ein. Manchmal gelingt es den Täterinnen und Tätern auch, die Website des Unternehmens zu übernehmen. Hier ist es besonders wichtig, die Sicherheitstipps zu beachten.
Wenn die Täter:innen die Kreditkartennummer und auch das Geburtsdatum haben, dann können sie z.B. bei einem Auktionshaus im Internet als Verkäufer:innen unter dem gestohlenen Namen auftreten und Waren verkaufen, die sie gar nicht haben. Den Ärger bekommt dann die Person, die wirklich so heißt und deren Kreditkarte angegeben wurde.

So kannst du dich schützen:

- ⇨ Niemals auf verdächtige E-Mails antworten, denn dadurch wissen die Betrüger:innen, dass die Adresse stimmt.
- ⇨ Passwörter, Kontonummern und Codes nie per E-Mail weiterschicken.
- ⇨ Wichtig ist, dass man in der Phishing-Mail keinen Link anklickt, da dieser womöglich zu einer gefälschten Internetseite führt.
- ⇨ Halte den Virenschutz des Computers auf dem neuesten Stand, damit keine gefährlichen Programme abgespeicherte Passwörter, Codes etc. vom Computer abfragen können.
- ⇨ Achte darauf, dass dein Internet Browser auf dem neuesten Stand ist und alle Updates durchgeführt wurden.
- ⇨ Kontrolliere immer die Adresse der besuchten Seite. Wenn z.B. www.testbank.at die richtige Adresse wäre, dann ist www.test-bank.at eine gefälschte Adresse.
- ⇨ Von einer Phishing-Mail kannst du immer dann ausgehen, wenn deine Kontonummer und Passwort abgefragt werden. Ein vertrauenswürdiges Unternehmen wird dies niemals tun!

Bild: SCHULDNERHILFE OÖ

Vorgang beim Phishing:

1. Die Betrüger:innen gestalten/kopieren eine Website (z.B. eines Bankinstitutes), die dem Original täuschend ähnlich sieht.

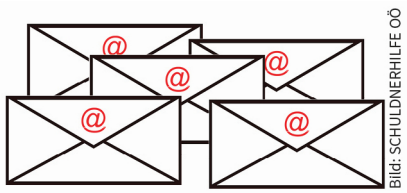

Bild: SCHULDNERHILFE OÖ

2. E-Mails werden an die Empfänger:innen verschickt, die zur Eingabe persönlicher Daten auffordern. Der (in der E-Mail angegebene) Link führt aber zur gefälschten Website.

Bild: SCHULDNERHILFE OÖ

3. Betrüger:innen hoffen nun, dass die persönlichen Zugangsdaten auf der gefälschten Website eingegeben werden. Von der gefälschten Website gelangen nun die Eingaben an die Betrüger:innen.

Bild: SCHULDNERHILFE OÖ

4. Mit den persönlichen Daten und Codes verschaffen sich die Betrüger:innen Zugang, wie z.B. zu Bankkonten, und können illegale Zahlungen veranlassen. Große finanzielle Schäden können auf diese Weise angerichtet werden.

vgl. www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/2/2/Seite.1720510.html (22.11.2022).