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.

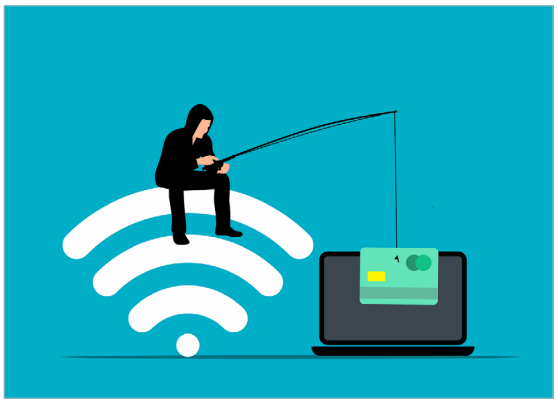

Bild: pixabay.com

Was ist daran gefährlich?

Die Methode ist fast immer gleich. Die Täter:innen senden E-Mails, Nachrichten über Messenger-Dienste wie WhatsApp oder SMS, die einen falschen Link (Verweis) zu einer Website enthalten. In der Nachricht 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 des richtigen Unternehmens, geben manche Leute ihre Daten ein. Manchmal gelingt es den Täter:innen auch, die Website des Unternehmens zu übernehmen. Hier ist es besonders wichtig, die Sicherheitstipps zu beachten.

So kannst du dich schützen:

- ➪ Bedenke, dass seriöse Unternehmen niemals per E-Mail oder in ähnlicher Form dazu auffordern, persönliche Daten wie Passwörter oder Transaktionsnummern bekannt zu geben. Klicke auf keine verdächtigen Links in E-Mails oder sonstigen Nachrichten.

- ➪ Antworte niemals auf Phishing-E-Mails, sondern lösche diese und informiere das Unternehmen, dessen Website hier offenbar für das Ausspionieren der persönlichen Nutzerdaten missbraucht wurde.

- ➪ Gib vertrauliche Daten ausschließlich über SSL-verschlüsselte Seiten bekannt. Diese sind beispielsweise am „https://“ und/oder dem geschlossenen Vorhängeschloss in der Adresszeile zu erkennen.

- ➪ Sei vorsichtig, wenn du eine Gewinnmitteilung erhältst, obwohl du an keinem Spiel teilgenommen hast.

- ➪ Prüfe Stellenangebote im Internet, die Finanzdienstleistungen (z.B. die Durchführung von Geldüberweisungen) zum Inhalt haben, besonders sorgfältig.

- ➪ Führe regelmäßig Sicherheitsupdates des von dir verwendeten Internetbrowsers durch.

vgl. www.oesterreich.gv.at/themen/onlinesicherheit_internet_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/2/2/Seite.1720530.html (6.11.2024)

Vorgang beim Phishing:

Bild: SCHULDNERHILFE OÖ

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

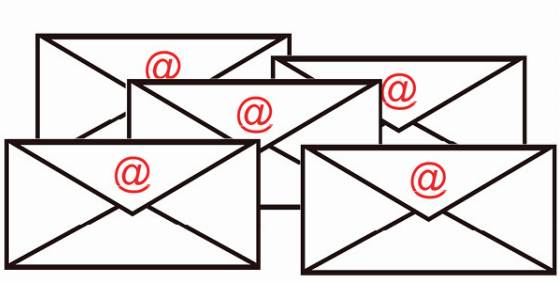

Bild: SCHULDNERHILFE OÖ

2. E-Mails oder andere Arten von Nachrichten (SMS, Nachrichten über Messenger-Dienste) werden an die Empfänger:innen verschickt, die zur Eingabe persönlicher Daten auffordern. Der (in der Nachricht 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 (04.11.2024).