23.10.2020

Aktuelle Phishing-Betrugsversuche

Seit dem Spätsommer haben Phishing-Nachrichten per E-Mail und SMS wieder markant zugenommen. Die Betrugsversuche werden dabei zusehends raffinierter. Lassen Sie sich nicht täuschen!

Internetkriminelle zeigen nicht nur technisches Verständnis, sondern immer wieder auch Einfallsreichtum. Waren während des Lockdowns noch Corona-bezogene Phishing-Nachrichten stark verbreitet, lassen sich die Betrüger seit August immer neue Maschen einfallen, um gutgläubige Nutzer hinters Licht zu führen: Angebliche Konto- und Kartensperrungen, zurückbehaltene Paketlieferungen, Lottogewinne, gewonnene Gutscheine und Rückerstattungen von Telekomdiensten gehören aktuell zu den beliebten Phishing-Fallen.

Die gefälschten Nachrichten erreichen die Anwender meist per E-Mail oder SMS – und werden immer glaubwürdiger. Die Angreifer schreiben in einwandfreiem Deutsch. Oft wird das Opfer mittels seiner eigenen E-Mail-Adresse oder gar seinem Namen angesprochen. Die Absender- Adresse wird ebenfalls oft gefälscht, und die verlinkte Phishing-Website verfügt häufig über HTTPS sowie einen Domain-Namen, der für den Laien oft als glaubwürdig einzustufen ist. Teilweise nutzen die Betrüger auch schadhafte E-Mail-Anhänge statt Links, um selbst erfahrene Empfänger in die Irre zu führen.

Vorsicht ist angesagt - keinesfalls aber Panik. Denn gegen all diese Betrugsversuche schützen ein paar einfache Verhaltensregeln:

- Nie einen Link verwenden, der per E-Mail, SMS oder Messenger-Dienst zugeschickt oder per QR-Code eingescannt wurde, um sich bei einem Finanzinstitut oder Online-Dienstleister anzumelden.
- Nie Formulare ausfüllen, die per E-Mail zugestellt wurden und zur Eingabe von Anmeldeinformationen auffordern.
- Anhänge von E-Mails und Kurznachrichtendiensten mit grosser Vorsicht behandeln.
- In Telefongesprächen nie vertrauliche Informationen, wie z.B. Passwörter, preisgeben.
- Die Adresse zur Anmeldeseite Ihres Online-Dienstleisters oder Finanzinstituts immer manuell in die Adresszeile Ihres Browsers eingeben.
- Beim Aufruf der Anmeldeseite die SSL-Verbindung (https://, Schlosssymbol) überprüfen und sich durch die Kontrolle der Internetadresse in der Adresszeile Ihres Browsers vergewissern, dass Sie sich am richtigen Ziel befinden.
- Sich bei Unsicherheit oder Unklarheit an das Finanzinstitut oder den Online-Dienstleister wenden.

Weitere Informationen finden Sie in unserem Artikel Phishing (https://www.ebas.ch/phishing) .