Betrügerischen Maschen rechtzeitig erkennen

Phishing – und wie man sich davor schützt

Phishing ist ein Kunstwort aus „Passwort“ und „fishing“ und steht für das Abgreifen oder Kopieren von persönlichen Daten und Passwörtern via E-Mail, Smartphone oder Brief. Sogenannte Datenfischer versuchen durch betrügerische Maschen an Kunden-Informationen zu gelangen, um diese gewinnbringend zu verkaufen.

Die gängigsten Arten von Phishing

Phishing per E-Mail

„Ihr Konto wurde vorübergehend gesperrt“ oder „Sie müssen Ihre Zugangsdaten aktualisieren“ – so oder ähnlich lauten meist die Betreffzeilen der E-Mails, die beim Phishing die Passwörter abgreifen wollen. Die dringend klingende Mail lockt über einen Link auf täuschend echt aussehende Kopien der originalen Internetseite. Hier sollen dann beispielsweise Geheimzahl (PIN) oder Einmalpasswort (TAN) eingegeben werden. Vermeintlich, um das eigene Konto wieder freizuschalten. Stattdessen erbeuten die Datenfischer hochsensible Informationen. Phishing-E-Mails enthalten zum Teil auch Anhänge. Diese können auf dem eigenen Gerät Schadsoftware installieren, die ebenfalls Daten abfängt oder zu einer Abo-Falle führt. Deshalb gilt: Niemals einen E-Mail-Anhang öffen, wenn man diesen nicht erwartet.

Phishing per SMS

Hier wird mithilfe irreführender SMS-Nachrichten dazu verleitet, wertvolle Informationen preiszugeben. Getarnt als Sparkasse oder Bank fordern Betrüger dazu auf, Daten zu aktualisieren oder etwas im eigenen Account zu überprüfen. Die SMS enthält oft einen Link zu einer Fake-Website, auf der Login-Daten eingegeben werden sollen. Dadurch kann dann die Kombination aus Nutzungsname und Passwort abgegriffen werden.

Wenn es darum geht, Geld zu stehlen, benötigen die Cyberkriminellen im Anschluss nur noch eine TAN. Dazu rufen sie manchmal sogar bei der betroffenen Person an, geben sich als Bankangestellte aus und fragen nach. Phishing-SMS können sowohl von einer unbekannten Nummer als auch von einer Nummer aus dem eigenen Adressbuch kommen. Im letzteren Fall könnte es sein, dass der entsprechende Kontakt selbst ein Opfer einer Betrugsmasche wurde.

Auf keinen Fall sollte einfach auf einen Link geklickt werden - egal, ob es sich um eine bekannte oder unbekannte Nummer handelt.

Thomas Mück
Leiter Marketing und Öffentlichkeitsarbeit
0911 / 7878 - 2401
presse@sparkasse-fuerth.de

Wichtig: Die Sparkassen verschicken in der Regel keine SMS-Nachrichten. Am besten man meldet sich telefonisch selbst in der Geschäftsstelle, ehe man auf Forderungen in einer SMS eingeht.

So kann man sich schützen

Am wichtigsten sind gesundes Misstrauen und Aufmerksamkeit. In manchen Fällen sticht einem die Phishing-Nachricht direkt ins Auge, in anderen Fällen muss man genauer hinsehen. Oft sind Betreffzeilen und Text in schlechtem Deutsch verfasst. Leider wird die Qualität jedoch immer besser, sodass sich ein Betrug nicht unbedingt auf den ersten Blick erkennen lässt.

Hat man eine verdächtige Mail erhalten, sollte der Blick direkt zum vermeintlichen Absender wandern. In manchen Fällen stimmt dessen Mail-Adresse beispielsweise gar nicht mit dem angeblichen Firmennamen überein. Wer Zweifel an der Echtheit einer Nachricht hat, sollte sich über eine seriöse Kontaktmethode direkt an den jeweiligen Absender wenden und nachfragen. Das ist bei Firmen meist über eine Telefonnummer auf der Webseite oder ein Kontaktformular möglich.

Was für die Mailadresse gilt, gilt auch für die Mobilfunknummer. Im Zweifel kann die Nummer bei Google eingegeben werden. Meist hatten auch andere schon Probleme mit der Nummer und konnten sie bereits als Fake melden.

Die Anrede ist in vielen Fällen unpersönlich: „Sehr geehrte/r Kundin/Kunde“. Aber Achtung: Mittlerweile kann die Anrede auch persönlich gestaltet sein und den eigenen Namen enthalten. Die eigenen Daten sollten heilig sein – und müssen auch so behandelt werden. Am besten verwendet man einen Passwortmanager. Dieser hilft dabei, Phishing zu umgehen.

Gefälschte Internetseiten haben in der Adresszeile des Browsers oft kein geschlossenes Schlosssymbol. Die Zeile beginnt dann mit „**http://**“ statt mit dem verschlüsselten „**https://**“. Allerdings leiten Betrüger mittlerweile auch auf sichere Websites mit https-Verschlüsselung über.

Schutz vor Phishing

Das Abfangen von Daten kann auch über öffentliches WLAN geschehen – das gibt es meist an Flughäfen, Cafés oder Einkaufszentren. Zwar wird das heutzutage durch die moderne Technik immer schwieriger, allerdings schaffen es Cyberkriminelle dennoch manchmal, den Datenverkehr mitzulesen. Unterwegs sollte deshalb immer ein virtuelles privates Netz (VPN) genutzt werden, um Informationen zu verschlüsseln. Das gilt besonders dann, wenn Bankgeschäfte erledigt werden.

Thomas Mück
Leiter Marketing und Öffentlichkeitsarbeit
0911 / 7878 - 2401
presse@sparkasse-fuerth.de

Online gibt es etliche Programme, die gegen Viren und Phishing-Angriffe schützen. Browser wie Chrome oder Firefox machen das, indem sie Nutzer gar nicht erst auf die schädliche Seite lassen.

Das gilt es im Betrugsfall zu tun

Ruhe bewahren und auf dem Endgerät die Zugangsdaten ändern. Betraf der Angriff die Bankdaten, sollte die Sparkasse informiert werden. Niemals die Phishing-Nachricht löschen, denn diese zählt als Beweismittel und kann bei strafrechtlicher Verfolgung wichtig sein.

Über die Sparkasse Fürth

Die Sparkasse Fürth bietet seit 1827 den Menschen in der Region alle Möglichkeiten für den Zahlungsverkehr, zum Sparen und zur Kreditaufnahme. Darüber hinaus sind das Wertpapiersparen, die Vermittlung von Versicherungen, Immobilien und Bausparverträgen aus der S Finanzgruppe wesentliche Geschäftsaktivitäten. Gelder werden primär im Geschäftsgebiet gesammelt und zur Entwicklung dieser Region wieder in Form von Finanzierungen zur Verfügung gestellt. Das Gemeinwohl und die langfristige Entwicklung stehen über einer kurzfristigen Gewinnerzielung.

Thomas Mück
Leiter Marketing und Öffentlichkeitsarbeit
0911 / 7878 - 2401
presse@sparkasse-fuerth.de