Was ist Phishing?

Und wie kann man sich davor schützen?

Klick! Und schon ist die Nachricht versendet. Klick! Überweisung erledigt. Klick! Die neuen Schuhe bezahlt. Keine Frage: Das Internet hat unser Leben vereinfacht. Leider auch das von Betrügern. Denn die nutzen die Möglichkeiten, die ihnen E-Mail, Websites, Internet-Telefonie und Messenger bieten, genauso und können dabei grossen Schaden anrichten. Phishing nennt man das. Und das betrifft nicht nur Privatpersonen. Phishing ist mittlerweile eine grosse Gefahr für Unternehmen.

Nur: Was ist Phishing? Und wie kann man sich davor schützen? Am besten durch Aufklärung. Bitte sehr:

Was bedeutet Phishing?

Unter Phishing versteht man die unrechtmässige Beschaffung von persönlichen Daten über gefälschte Websites, E-Mails oder Kurznachrichten mit dem Ziel, das Konto des Bestohlenen zu plündern und ihm anderweitig persönlich zu schaden. Phishing ist ein englisches Kunstwort, das sich aus «password harvesting» (Passworte sammeln) und «fishing» (Angeln, Fischen) zusammensetzt und somit das Angeln nach Passwörtern mit Ködern darstellt.

Wie funktioniert Phishing?

Durch eine Fälschung erstellen die Betrüger eine identisch aufgestellte Webseite einer vertrauenswürdigen Institution: einer Bank, eines E-Mail-Providers oder einer Shopping-Seite. Der User wird beim Phishing auf dieser gefälschten Seite dazu aufgefordert, sich einzuloggen oder seine Daten für das Online-Banking einzugeben. Diese Daten werden dann «abgefischt» bzw. gesammelt und dazu missbraucht, um sich vom Userkonto ungerechtfertigt zu bereichern. Phishing ist eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird. Oft indem E-Mails mit gefälschten Absenderadressen zugesandt werden.

Phishing-Mails

Sie kommen wie offizielle Nachrichten daher: Phishing-E-Mails behaupten, dass die Zugangsdaten oder Kontoinformationen des Empfängers abgelaufen oder nicht mehr sicher seien und dass der Empfänger diese Daten sofort unter einem angehängten Link ändern solle. Dieser Phishing-Link führt dann zu einer Phishing-Website, die identisch mit einer Dienstleistungsanbieter-Website ist, auf der dann diese Informationen «abgefischt» bzw. gesammelt und den Betrügern übermittelt werden.

Was sind die Gefahren bei Phishing?

Hat der Betrüger Bankdaten über die Phishing-Website abgefischt, kann er nach Belieben das Konto leeren, die Kreditkarte missbrauchen oder online einkaufen.

Mit Zugangsdaten für E-Mail-Konten kann er private Daten auslesen oder betrügerische Nachrichten an die Kontakte schicken sowie diese um Geld oder Gefallen bitten.

Ausserdem besteht die Gefahr, dass mit dem Anklicken eines Phishing-Links eine Schadsoftware heruntergeladen wird, die den Rechner ausspioniert, unbrauchbar macht oder im schlimmsten Fall verschlüsselt. Mit einem sogenannten Verschlüsselungstrojaner, oder auch Erpressungstrojaner werden die Dateien auf dem betroffenen Computer und allen mit ihm verbundenen Laufwerken verschlüsselt und somit für das Opfer unlesbar gemacht. Für Unternehmen ist das gleich doppelt übel, denn der Geschäftsbetrieb wird nicht nur auf unbestimmte Zeit unterbrochen. Der Erpresser verlangt auch eine hohe Summe für die Freigabe der Daten. Und das kann existenziell werden.

Phishing betrifft nicht nur Privatpersonen, sondern ist eine grosse Gefahr für Unternehmen. Mit schwerwiegenden Folgen.

Wie erkenne ich ein Phishing-Mail?

So unterschiedlich Phishing-Attacken auch ablaufen, an diesen zehn typischen Merkmalen erkennen Sie ein Phishing-Mail:

1. Sie kennen den Absender nicht.
2. Sie werden nicht persönlich angesprochen («Sehr geehrter Kunde»).
3. Das E-Mail fordert Sie zu einer dringenden Handlung auf («Loggen Sie sich innerhalb von 2 Tagen ein.»).
4. Das E-Mail enthält Drohungen («Andernfalls wird Ihr Konto gesperrt.»).
5. Der Text ist in schlechtem oder fehlerhaftem Deutsch geschrieben.
6. Umlaute wurden vergessen oder aufgelöst (statt «ü» steht «u» oder «ue»).
7. Ihre vertraulichen Daten werden abgefragt.
8. Die URL beginnt nicht mit https://.
9. Die URL enthält verdächtige Zeichen (69z-allianz.ch oder az-suisse.kunden.ch).
10. Auf der verlinkten Website fehlt das SSL-Sicherheitszertifikat (Secure Socket Layer).

So schützen Sie sich gegen Phishing

Die Tricks der Betrüger sind zwar raffiniert, aber wenn Sie auf die folgenden acht wichtigen Regeln zur Prävention gegen Phishing achten, dann können Sie die Betrüger umgehen:

1. Misstrauen Sie E-Mails, deren Absenderadresse Sie nicht kennen. Besonders vertrauenswürdige Unternehmen werden gerne gefälscht.
2. Seien Sie vorsichtig, wenn Sie E-Mails bekommen, die eine Aktion von Ihnen verlangen und mit Konsequenzen drohen (Geldverlust, Strafanzeige, Konto- oder Kartensperrung usw.)
3. Überprüfen Sie Zahlungsaufforderungen, die Sie per E-Mail erhalten.
4. Klicken Sie in verdächtigen E-Mails auf keine Anhänge und keinen Link.
5. Öffnen Sie keine E-Mail-Anhänge mit skurrilen Endungen (z. B. picture.bmp.vbs).
6. Besuchen Sie nur vertrauenswürdige Websites.
7. Kontrollieren Sie regelmässig Ihre Kreditkartenabrechnungen und Bankauszüge.
8. Schützen Sie Ihre Computer mit Antiviren-Programmen, und halten Sie Ihre Software immer auf dem neuesten Stand.

GUT ZU WISSEN

Seriöse Dienstleister fordern ihre Kundinnen und Kunden niemals mit einem E-Mail oder einer Kurznachricht zur Angabe von Passwörtern oder Kreditkartendaten auf.

Was ist Phishing und wie erkenne ich ein Phishing-Mail? | Allianz