Merkblatt

SKS stärkt die Konsumenten

Bern, 03. Mai 2016

Phishing – Abzocke per E-Mail und Internet

Heute ist den meisten Computerbenutzern bewusst, dass von verdächtigen E-Mails eine gewisse Gefahr ausgeht. Nichts Anklicken, nicht beantworten und direkt löschen, lautet die Devise. Doch welchen Hintergrund haben diese E-Mails? Was passiert, wenn Sie darauf reagieren?

Welche Gefahr geht von E-Mails aus?

Phishing

Jeden Tag werden unzählige E-Mails verschickt, welche nur einen Zweck haben: Gutgläubigen Menschen das Geld aus der Tasche zu ziehen. Durch **E-Mails mit gefälschten Absenderangaben** versuchen Betrüger, Passwörter und andere sensible Daten zu erlangen, um ihre Opfer per E-Banking, bei anderen Internetdiensten oder mit Kreditkartendaten **finanziell zu schädigen**.

Dabei sollen Sie sensible Daten entweder direkt in einer Antwort-Mail senden oder auf einen Link klicken und sich dort – auf einer **gefälschten Webseite** – einloggen.

Es werden nicht nur Banken als Absender gefälscht, sondern auch beliebige andere Anbieter, bei welchen man sich mit Benutzerdaten einloggen muss – etwa Auktionsplattformen, soziale Medien oder Telekomanbieter.

Dieses Vorgehen wird Phishing genannt. Die Begriffsherkunft ist nicht restlos geklärt, setzt sich aber womöglich aus den englischen Wörtern für Passwort („password“) und fischen („fishing“) zusammen.

Schadsoftware

Der unvorsichtige Umgang mit E-Mails birgt zudem eine weitere Gefahr: Durch das Klicken auf Links oder das Öffnen von Dokumenten können Viren und andere Schadsoftware auf dem Computer installiert werden. Solche Programme werden unter anderem dazu verwendet, um die Betroffenen finanziell zu schädigen.

Wie erkenne ich verdächtige E-Mails?

Eine Phishing-Mail kann eines oder mehrere der folgenden Merkmale aufweisen:

- Die E-Mail ist in einer anderen Sprache oder schlechtem Deutsch verfasst.
- Die E-Mail kommt von einem unbekannten Absender (z.B. von einer Bank, bei welcher Sie nicht Kunde sind).
    - Achtung: Die Mails können auch von bekannten Absendern kommen und in perfektem Deutsch verfasst sein.
    - Die Täter fälschen teilweise die Identität von Menschen, die die Opfer persönlich kennen. Notwendige Daten finden Abzocker z.B. auf Facebook.

Merkblatt

SKS stärkt die Konsumenten

- Manchmal verrät schon ein Blick auf die E-Mail-Adresse des Absenders, dass es sich um eine Fälschung handelt.
- Der Absender der E-Mail teilt Ihnen mit, dass mit Ihrem Konto, Ihren Zugangsdaten, Ihren Transaktionen o.ä. etwas nicht stimmt.
- Der Absender der E-Mail fordert Sie dazu auf, Ihr Passwort und/oder andere sensible Daten anzugeben.
- Der Absender fordert Sie dazu auf, auf einen Link zu klicken und sich dort einzuloggen.

Wie schütze ich mich vor einem Betrug?

- Misstrauen Sie E-Mails, welche Sie unaufgefordert bekommen.
- Löschen Sie verdächtige E-Mails.
- Klicken Sie keine Links an und öffnen Sie keine Dokumente.
- Loggen Sie sich nicht auf externen Webseiten ein, auch wenn Sie echt aussehen.
- Antworten Sie nicht auf die E-Mails.
- Wenn Sie nicht sicher sind, ob es sich um eine echte Nachricht handelt: Fragen Sie beim Absender nach. Tun Sie dies über eine offizielle Telefonnummer oder E-Mail-Adresse.

Was tun, wenn ich bereits reagiert habe?

Wenn Sie auf einen Phishing-Versuch reagiert haben – z.B. indem Sie sich auf einer verlinken Seite eingeloggt haben:

- Melden Sie den Vorfall den betroffenen Dienstleistungsanbietern (Bank, Kreditkartenanbieter, E-Mail-Dienst etc.) und klären Sie ab, was zu tun ist.
- Ändern Sie Ihre Zugangsdaten sofort überall, wo Sie dieselben Daten verwenden.

Was, wenn ich finanziell geschädigt wurde?

- Wenden Sie sich an das Finanzinstitut, welches die Transaktion durchgeführt hat.
- Wenden Sie sich für strafrechtliche Schritte an die Polizei.

Wo kann ich Betrugsversuche melden?

- Gefälschte Webseiten: https://www.antiphishing.ch/de/
- Phishing-Mails können Sie direkt an die Adresse *reports@antiphishing.ch* weiterleiten.
- Meldeformular der Bundespolizei für kriminelles oder verdächtiges Verhalten im Internet.
- Sie helfen damit, weitere Betrugsversuche zu verhindern

Weitere Informationen

- Webseite des KOBIK (Koordinationsstelle gegen Internetkriminalität)
- Webseite von MELANI (Melde- und Analysestelle Informationssicherung)
- Wikipedia
- SKS-Miniratgeber „Vorsicht Betrug!“

Hat Ihnen dieses Merkblatt geholfen?
Um unser Angebot ausbauen und unterhalten zu können, sind wir auf Ihre Unterstützung angewiesen.
Gönnerschaft / Förderschaft / SMS-Sofortspende / Postkonto: 30-24251-3.
Gönner und Förderer beraten wir kostenlos. Herzlichen Dank!