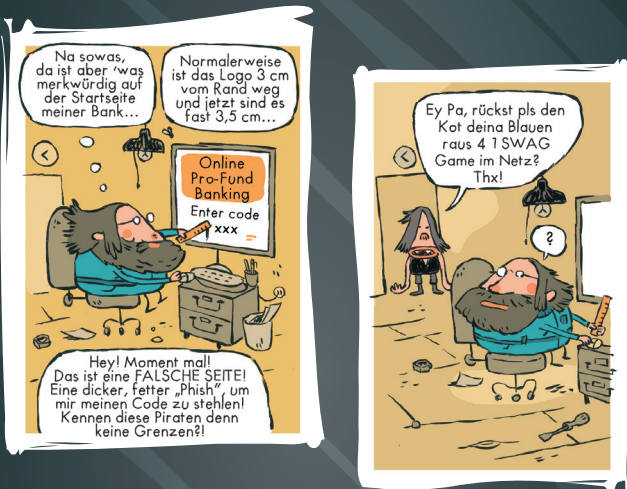


PHISHING



Toundra



SZENARIO

Sie erhalten eine E-Mail von Ihrer Bank oder einem anderen Online-Dienst, bei dem Sie angemeldet sind. Daraus geht hervor, dass es offensichtlich Probleme mit Ihrem Konto gibt. Was genau passiert ist, bleibt unklar. Dringend werden Sie jedoch dazu aufgefordert, sich in Ihren Account einzuloggen, um „das Schlimmste zu verhindern“. Praktisch, dass der Absender den passenden Link gleich mitliefert. Sie brauchen ihn nur noch anzuklicken und gelangen gleich auf eine Seite, auf der Sie sich einloggen sollen.

Das Problem dabei: Die Seite, auf die Sie über den Link gelangen, sieht ihrem offiziellen Pendant zwar täuschend ähnlich, ist aber gefälscht. Alle Daten, die Sie hier eingeben, werden von Kriminellen gespeichert und anschließend für kriminelle Zwecke verwendet bzw. verkauft.

Phishing bezeichnet eine Form des Online-Betrugs, die darauf abzielt, User zu täuschen und sie dazu zu verleiten, Login-Daten preiszugeben, die der Angreifer anschließend nutzt, um sich die Nutzerrechte des Opfers anzueignen und sie zu seinem persönlichen Vorteil zu benutzen.

GEWINN DES ANGREIFERS

- Finanzielle Bereicherung (E-Banking, E-Commerce,...)
- Identität des Opfers, um Schadsoftware zu verbreiten oder Kontakte des Opfers zu betrügen
- Geheimnisse aus Industrie, Diplomatie, Militär
- Wirtschaftliche Vorteile
- Sabotage der Konkurrenz

Phishing-Mails kursieren in allen Sprachen und Variationen. Einige wirken äußerst primitiv, strotzen vor Rechtschreibfehlern und machen schon allein dadurch skeptisch. Andere jedoch sind nahezu perfekt aufgesetzt, mit den Logos der Originalseite und scheinbar vertrauensvollen Links und sind selbst für IT-Spezialisten schwer zu enttarnen.

KONSEQUENZEN FÜR DAS OPFER

- Kontrollverlust
- Ruf- und Imageschäden
- Direkte finanzielle Verluste
- Zusätzliche Arbeitszeit
- Produktionsstörung
- Einstellung der Aktivität
- Verbreitung von Geheimnissen
- Verlust von Glaubwürdigkeit
- Identitätsdiebstahl

Cyberkriminelle versenden Phishing-Mails oft an Millionen Empfänger weltweit. Dabei haben sie meist kein spezifisches Ziel und wissen nicht, wer genau ihr Opfer wird. Sie bauen darauf, dass je mehr E-Mails versendet werden, umso mehr Empfänger darauf hereinfallen.

DIE AUSGENUTZTE SCHWACHSTELLE

Beim Phishing klickt das Opfer freiwillig auf einen Link in einer ungebetenen E-Mail. Die Masche funktioniert also aufgrund der Leichtgläubigkeit und Arglosigkeit der Internetbenutzer und basiert auf vier Prinzipien:

- 1 Die Cyberkriminellen geben sich als ein offizielles und vertrauenswürdiges Unternehmen aus, um personenbezogene Daten zu erhalten, indem eine Nachricht (E-Mail) geschickt wird.
- 2 Unter falschem, oft dringendem Vorwand werden die Empfänger in dieser Nachricht darum gebeten, persönliche Informationen mitzuteilen.
- 3 Die Opfer werden auf eine eigens dafür vorbereitete, aber der offiziellen Internetseite optisch sehr ähnlichen Webseite weitergeleitet, damit sie dort die gefragten Informationen eingeben.
- 4 Die eingegangenen Informationen werden verwendet, um sich als das Opfer auszugeben, mit dem Ziel, Sachwerte und Dienstleistungen zu erhalten.

SCHUTZMAßNAHMEN

Klicken Sie nicht auf Links in E-Mails. Am sichersten ist es, Webadressen manuell in die Adresszeile des Browsers einzutippen.

Tipp: Einen kompromittierten Link enttarnen Sie in vielen Fällen, indem Sie mit dem Mauszeiger darüber fahren, ohne zu klicken. Das wahre Ziel des Links wird dann vom E-Mail-Programm angezeigt. Doch Vorsicht: Auch wenn der Link legitim wirkt, kann es eine bewusste Täuschung des Angreifers sein.

Geben Sie keine personenbezogenen Informationen in Formulare ein, die per E-Mail eintreffen.

Antworten Sie nicht auf E-Mails, in denen vertrauliche oder personenbezogene Informationen angefordert werden.

Versenden Sie keine persönlichen Daten per E-Mail. Jeder kann mit einfachen technischen Mitteln auf den Inhalt der Korrespondenz zugreifen.

Außerdem sollte jede E-Mail kritisch geprüft werden. Besondere Vorsicht gilt, wenn:

Eine E-Mail Sie unter Druck setzt, schnell zu reagieren (da sonst etwa Ihre Kreditkarte gesperrt oder Ihr Konto gelöscht würde).

Eine E-Mail Sie dazu auffordert, einen Link anzuklicken, um auf eine Webseite zu gelangen, wo Sie Ihre Daten eingeben sollen.

Eine E-Mail nicht an Sie persönlich gerichtet ist oder viele Schreibfehler, bzw. eine sehr schlechte Übersetzung enthält. (Wobei auch eine persönliche Anrede kein Garant für eine vertrauenswürdige E-Mail ist!)

Seriöse Unternehmen würden niemals vertrauliche Informationen anfordern, insbesondere nicht per E-Mail. Falls die Herkunft einer Mail unklar ist, sollten Sie direkt mit dem Absender-Unternehmen telefonischen Kontakt aufnehmen, um die Echtheit zu prüfen.



Toundra

SOS - WAS TUN, WENN ES PASSIERT?

- Versuchen Sie, so schnell wie möglich das Passwort im legitimen Online-Dienst zu ändern, eventuell mit Zuhilfenahme der Geheimfrage.
- Falls dies nicht mehr geht, kontaktieren Sie den Online-Dienst und lassen Sie das Konto sperren, bzw. über diesen Weg das Passwort zurücksetzen.
- Kontaktieren Sie den Betreiber des legitimen, im Phishing missbrauchten, Online-Dienstes und informieren Sie ihn über den Phishing-Angriff (es gibt sicher weitere Opfer).
- Falls das gestohlene Passwort bei anderen Online-Diensten verwendet wurde, ändern Sie unbedingt auch diese Passwörter.

Weitere Tipps zur Informationssicherheit:

www.cases.lu · help@cases.lu