Sicherheitsmassnahmen
für den Schutz gegen Phishing-Attacken

Folgende Regeln sind strikt zu befolgen, um Schäden im Falle einer Phishing-Attacke zu minimieren:

1. Nicht jedem E-Mail blind vertrauen

Eine schöne Formatierung und korrekte Rechtschreibung sind keine Anzeichen, dass die E-Mail wirklich vom angegebenen Absender stammt. Vorsicht ist vor allem bei E-Mails geboten, die Anhänge und Links beinhalten.

2. Verifiziere den Absender des E-Mails

Bei E-Mail-Adressen spielt es keine Rolle, was vor dem @-Zeichen steht, denn dies lässt sich ganz einfach fälschen. Man muss immer die Angabe nach dem @-Zeichen überprüfen. Aber auch da wird getrickst - beispielsweise werden Buchstaben mit Zahlen vertauscht (O und 0) oder sehr ähnliche Adressen erstellt (z.B. @microsof.com). Immer sehr genau hinsehen und im Zweifelsfalle den Absender anrufen.

3. Bei einem E-Mail mit Anhang: Überprüfe den Anhang

Prüfe immer die Dateiendung des Anhanges, bevor Du ihn öffnest. Phishing-Attacken werden oft über Word oder Excel Dateien verübt (.doc/.docx/.xls/.xlsx). Diese können Makros enthalten, die beim Klicken Malware installieren. Weitere potenziell gefährliche Dateien sind: .ppt, .pptx, .zip, .rar, .exe.

PS: Sofern Dateien nicht intern weiterbearbeitet werden müssen, sollte man diese immer als PDF versenden. „Offene“ Word und Excel Dateien zu versenden ist unprofessionell und birgt grössere Risiken.

4. Bei einem E-Mail mit einem Link: Überprüfe die Internetadresse

Auch über ein Link im E-Mail kann eine Datei heruntergeladen werden. Falls etwas heruntergeladen wird, die Datei keinesfalls öffnen und den Vorfall umgehend melden. Falls Du unsicher bist, ob Du etwas ausgeführt hast, schalte den Computer aus.

Falls der Link auf eine Webseite führt: Kontrolliere, ob es sich um eine sichere Seite handelt (sieht man am «https:\\» oder am Schlosssymbol vor dem Link). Achte dich auch darauf, ob die Webadresse wirklich eine offizielle Seite des vorgegebenen Unternehmens ist. Wenn Du unsicher bist, suche die Unternehmenswebsite über Google und vergleiche die beiden Internetadressen.

Wenn Du doch geklickt hast

Falls Du eine E-Mail im Postfach hast, die potenziell gefälscht ist, oder Du sogar eine Datei heruntergeladen oder Dein Passwort eingegeben hast, sind folgende Schritte umgehend einzuleiten:

1. Bei Passworteingabe: Ändere umgehend Dein Passwort

Dies ist der wichtigste Schritt, denn wenn das Passwort umgehend geändert wird, kann man die Gefahr schon gut bannen. Wenn Du das Passwort nicht änderst, kann der Hacker damit z.B. Deine Daten einsehen, Deine E-Mails lesen oder sogar E-Mails in Deinem Namen verschicken. Auch solltest Du überall das Passwort ändern, wo Du es sonst noch verwendet hast (man sollte ein Passwort übrigens nie mehrmals verwenden, by the way!)

2. Bei Download einer Software: Abbrechen und NICHT ausführen

Wenn möglich, den Download sofort abbrechen. Falls die Datei bereits heruntergeladen ist, die Datei keinesfalls öffnen und ausführen!

3. Immer: Melde dich bei deinem IT Verantwortlichen

Wenn ein Phishing-Mail sofort gemeldet wird, lässt sich der Schaden gut eindämmen. Die IT Abteilung kann dann nämlich sofort alle Mitarbeiter informieren und vorwarnen.

4. Niemals: E-Mail Adresse und Passwort irgendwo eingeben

Seriöse Dienstleister wie Banken, Post, Online-Auktionsanbieter, Behörden und andere Institutionen werden dich nie über E-Mail zur Angabe von Passwörtern oder Kreditkartendaten auffordern. Sei deshalb immer misstrauisch, wenn in einem E-Mail persönliche Daten verlangt und mit Konsequenzen wie Geldverlust, Strafanzeige oder Kartensperrung gedroht wird.

Entec ist Ihr IT-Partner für Infrastruktur, Sicherheit oder Full-IT-Outsourcing

Falls Sie weitere Fragen zur IT Sicherheit haben oder interessiert sind an einem professionellen Phishing-Schutz aus der Cloud, wenden Sie sich jederzeit an unsere Security Experten unter: 044 800 80 00 oder info@entec.ch.