Wie Sie betrügerische E-Mails, Textnachrichten und Anrufe erkennen – und richtig reagieren

Phishing: Gehen Sie den Betrügern nicht ins Netz

Per E-Mail können wir sekundenschnell Informationen mit Personen in aller Welt austauschen. Das hat allerdings seinen Preis: Cyberkriminelle können genauso leicht mit Ihnen in Kontakt treten. Wir sprechen hier von sogenannten "Phishing"-E-Mails.

Dabei erhalten Sie scheinbar legitime E-Mails, in denen Sie aufgefordert werden, bestimmte Angaben zu machen, einen Link anzuklicken oder einen Anhang zu öffnen. Die Betrüger "fischen" so nach Ihren Daten. Außerdem können Cybergangster auf diesem Weg Malware auf Ihren Geräten installieren, Ihre Daten stehlen und sogar "Lösegeld" von Ihnen fordern.

So können Sie sich schützen:

Hinterfragen Sie jede unverlangte Kontaktaufnahme

Seien Sie auf der Hut vor unerwarteten E-Mails, Anrufen oder Faxmitteilungen. Besonders wenn Sie als Kunde von einem Dritten oder eines Online-Anbieters kontaktiert werden. Sollte Ihnen der Absender, Anrufer oder Grund der Anfrage zweifelhaft erscheinen, geben Sie niemals vertrauliche Informationen preis. Wenn Sie im Namen von «GEHE» eine fragwürdige Mitteilung erhalten, kontaktieren Sie uns bitte.

Klicken Sie bei verdächtigen E-Mails nicht auf Links und öffnen Sie keine Anhänge

Es ist nicht immer einfach, eine seriöse E-Mail von einer Phishing-E-Mail zu unterscheiden. Achten Sie auf untypische Absenderadressen, Schreibfehler, Tonalität, Haftungsausschlüsse und Logos der E-Mail. Klicken Sie im Zweifelsfall nicht auf Links und öffnen Sie keine Anhänge.

Besuchen Sie nur vertrauenswürdige Webseiten

Steht https:// vor der Adresse, handelt es sich um eine sichere Webseite. Speichern Sie Webseiten, die Sie häufig besuchen, unter Ihren Favoriten. Füllen Sie niemals Webformulare mit vertraulichen Daten aus, wenn Sie Zweifel an der Vertrauenswürdigkeit der Webseite haben. Wichtig zu wissen: «GEHE» verschickt niemals E-Mails mit Links zu Login-Seiten.

Überprüfen Sie Zahlungsaufforderungen, die Sie per E-Mail erhalten

Sollten Sie Bankangaben für eine Zahlung per E-Mail erhalten, überprüfen Sie diese stets mit dem Empfänger. Kontaktieren Sie diesen dazu auf einer offiziellen Nummer – und wählen Sie nicht die Nummer, welche auf der E-Mail aufgeführt ist.

Ignorieren Sie E-Mails über angeblich ungewöhnliche Kontobewegungen

Phishing-E-Mails wollen erreichen, dass Sie einen bestimmten Link anklicken oder Anhang öffnen. Dazu wird absichtlich Neugier, Angst oder Handlungsdruck provoziert. Vertrauenswürdige Gesellschaften informieren Sie hingegen kaum per E-Mail über ungewöhnliche Transaktionen. Löschen Sie verdächtige E-Mails und leeren Sie den Papierkorb des betreffenden Programms. Direkt abblocken können Sie E-Mails dieser Art auch mit einem Spamfilter.

Halten Sie Ihre Software auf dem neusten Stand

Aktualisieren Sie Ihr Antivirenprogramm regelmässig für noch besseren Schutz. Auch Spamfilter und sogar «Anti-Phishing»-Software helfen, Phishing Webseiten und E-Mails herauszufiltern.