Kenne die Warnsignale eines Phishing Angriffs

security@deinebank.example.com
Dringend! Ihr DeineBank Konto wird geschlossen!
To: deine.emailadresse@deinedomain.com

DeineBank

Sehr geehrter Kunde,

Leider werden in letzter Zeit Bankkonten von Kriminellen gekapert und ohne Wissen der Besitzer für illegale Transaktionen missbraucht.
Auf Ihrem Konto gab es verdächtige Aktivitäten und es wird in Kürze gesperrt.

Sie müssen dringend Ihre Konto Informationen aktualisieren .Sonst wird Ihr Konto von der Polizei beschlagnamt.

1. Aktualisieren Sie Ihre Informationen jetzt. Es dauert nur eine Minute.
2. Bestätigen Sie, dass das Konto Ihnen gehört.

Hier geht es zu Ihrem Konto:
http://account.deinebank.example.com

Vielen Dank für Ihr Verständnis,

DeineBank AG
Security Abteilung

Herrengasse 66
9490 Vaduz
Liechtenstein
www.deinebank.li

< seltsame E-mailadresse und falsche Domain des Absenders

< Branding und Layout authentisch?

< unpersönliche Anrede, deine E-Mailadresse oder keine Anrede

< angebliches Account Problem

< Handlungsdruck
< Rechtschreibung

< Irreführender Link, unbekannte Domain
Machmal ist der tatsächliche Link hinter Text verborgen
Mouseover macht tatsächlichen Link sichtbar
http:// statt https:// -> Finger Weg!

< Firmenname/Absender authentisch?
Banken versenden keine E-Mails

Unpersönliche Anrede

Da Phishing-E-Mails massenhaft verschickt werden, verwenden sie oft allgemeine oder keine Begrüssungsformeln (Hallo; Guten Tag; Lieber Kunde; etc.). Manchmal ist deine E-Mail-Adresse die Begrüssung.

Seltsame E-Mail-Adresse

Eine E-Mail von sicherheit@d**ie**nebank.li gaukelt vor, dass es sich um eine legitime Nachricht von @d**ei**nebank.li handelt. Das Gehirn sieht oft nur, was es erwartet und lässt sich so leicht täuschen.

Problem mit deinen Account-Informationen

Mit deinem Account (Bank, Shop, Spedition, Social-Media) stimmt etwas nicht und du sollst Deine Konto-Daten bestätigen. Der Link im Mail führt zu einer gefälschten Anmeldeseite, die Deine Anmeldedaten stiehlt. Wenn du nicht sicher bist, wende dich telefonisch an den Dienstanbieter oder ruf in einem neuen Browserfenster die echte Website des Anbieters auf.

Handlungsdruck

Das Opfer wird bedrängt, auf einen schädlichen Link oder Mailanhang zu klicken. Mit Social-Engineering-Tricks werden Emotionen wie Angst, Aufregung oder Gier geschürt und zu sofortigem Handeln aufgefordert. Dieser Handlungsdruck ist ein wichtiges Warnsignal!

E-Mail-Anhang

E-Mail-Anhänge können Schadcode enthalten. Wird der Anhang geöffnet, kann sich ein Schadprogramm auf dem Computer einnisten. Erwartest du beim E-Mail überhaupt einen Anhang? Frag nach, wenn du nicht sicher bist.

Du hast etwas gewonnen!

Zu schön, um wahr zu sein. Die Erwartung eines vermeintlichen Gewinns trügt die Urteilskraft. Frage dich, ob die Nachricht plausibel ist. Bist du unsicher, geh in einem neuen Browserfenster auf die Website des bekannten Absenders oder ruf an. Das gilt auch bei unerwarteten E-Mails zu Gutschriften und Rückerstattungen.

Irreführende Links im Text

Um den Link zu überprüfen, schiebe den Mauszeiger ohne zu klicken über den Link (*Mouseover*). Jetzt wird die tatsächliche Ziel-URL eingeblendet. Achte auf kleinste Fehler in der URL, wie kleine Schreibfehler oder Buchstaben, die mit Ziffern ersetzt wurden, ein zusätzlicher Punkt. Die Adresse www.deinebank.example.com führt nicht zu einer Unterseite von deinebank.com, sondern zu einer von example.com

Rechtschreibung und Sprache

Viele Phishing-Mails sind maschinenübersetzt oder einfach schlecht geschrieben. Achte auf Rechtschreibfehler und seltsame Sätze. Passt die Sprache zum Absender? Phinshing wird immer professioneller. Auch Angreifer verwenden ChatGPT und Co. um gute Texte zu erstellen oder um den Stil einer Firma/Person nachzuahmen.

Smishing und Vishing

Phishing-Angriffe gibt es auch als SMS (Smishing) und übers Telefon (Vishing). Es gelten dieselben Regeln: Misstrauisch sein, nicht unter Druck setzen lassen. Allenfalls über eine bekannte Telefon-

Sei misstrauisch, prüfe immer!

Achte auf die Warnsignale und klick auf keine Links und Anhänge, wenn du unsicher bist. Lass dich nicht unter Druck setzen! Besonders gefährlich sind Phishing-Mails, die betriebsintern an Dich zur Bearbeitung weitergeleitet werden, weil sie jetzt von einem seriösen Absender kommen.

BÜRO MARXER

Cloud Solutions
Managed Security
Document Solutions

Büro Marxer AG
Im alten Riet 38
LI-9494 Schaan

T+423 239 09 09
info@bueromarxer.com
www.bueromarxer.com