

PHISHING E-MAILS

Phishing E-Mail erhalten?

Aufgrund der anhaltenden Bedrohung durch Malware, welche sehr oft via Phishing E-Mails verteilt wird, sind proaktive Massnahmen zum Schutz von Unternehmen und Organisationen unabdingbar geworden. Vulnerability- und Patch-Management Konzepte reduzieren das Gesamtrisiko bezüglich Malware-Infektionen bereits erheblich. Ein weiterer, wichtiger Schritt zur Risikominderung ist auch die proaktive Erkennung von Phishing E-Mails durch die Mitarbeitenden. Wie Sie Phishing E-Mails erkennen können, lesen Sie in den folgenden 10 Merkmalen:

- 1 Vertrauen Sie nicht dem angezeigten Absender.** Nur weil da steht, es kommt von jemandem, den Sie kennen oder vertrauen, heisst nicht, dass dem auch so ist. Überprüfen Sie die Absender-Adresse genau.
- 2 Schauen, aber nicht klicken.** Fahren Sie mit dem Cursor über Links oder Anhänge in der E-Mail, ohne auf etwas zu klicken. Entspricht die Kennzeichnung oder Beschreibung nicht dem Link respektive dem Anhang, klicken Sie nicht darauf – melden Sie es.
- 3 Achten Sie auf Rechtschreibfehler.** Angreifer sind oft weniger an korrekter Rechtschreibung, Satzbau oder Stilistik interessiert als normale, vertrauliche Absender.
- 4 Berücksichtigen Sie die Anrede.** Werden Sie hellhörig, wenn die Anrede gewöhnlich oder unüblich bzw. unbestimmt ist. Lautet die Anrede «Sehr geehrte/r Frau/Herr», einfach nur «Hi/Hallo» oder gar «Liebe/r Herr/Frau [Name hier eintragen]», so ist ebenfalls Vorsicht geboten.
- 5 Wird nach persönlichen Informationen gefragt?** Vertrauenswürdige Firmen resp. deren Absender fragen in E-Mails eher selten nach persönlichen Informationen.
- 6 Überprüfen Sie die Signatur der E-Mail.** Die meisten, vertrauenswürdigen E-Mails haben eine komplette und korrekte Signatur am Ende ihrer Nachricht.
- 7 Achtung bei Dringlichkeit.** Gewisse E-Mails machen den Eindruck, es sei ein Notfall. Beispiele sind plötzliche Überweisungen für jemanden aus der Geschäftsleitung oder jemand anderes benötigt mal wieder dringend Hilfe.
- 8 Vorsicht mit Anhängen.** Angreifer versuchen, mit reizvollen Anhängen zu ködern. Lange Dateinamen oder falsche Symbolbilder sind Indikatoren. Ein falsches Excel-Symbol ist mitunter nicht die Tabelle, die Sie erwarten.
- 9 Glauben Sie nicht alles, was Sie sehen.** Scheint auch nur ein kleiner Teil einer E-Mail etwas merkwürdig, gehen Sie besser auf Nummer sicher, als sich später entschuldigen zu müssen. Geben Sie am besten gleich Ihrer IT Bescheid.
- 10 Unsicher? Melden Sie es.** Egal zu welcher Zeit oder zu welchem Anliegen. Lieber einmal mehr etwas Unscheinbares melden, als Ihr Unternehmen einem unnötigen Risiko auszusetzen.



Ihr Netcloudpartner:
Franck Bouchoux

Benötigen Sie Hilfe? Erfahren Sie mehr über unsere Cyber Defence Services und melden Sie sich:
bouchoux@netcloud.ch