Phishing: Gefälschte E-Mails, Webseiten und Co.

#it-security #phishing #e-mails #kommunikation #covid19 #noemedia

Mit dem Begriff Phishing (Password fishing) wird der Versuch beschrieben, die **persönlichen Daten** von Nutzern illegal zu „**angeln**“. Sensible Daten, wie zum Beispiel Zugangsdaten, Passwörter oder Kreditkartennummern der Nutzer*innen kommen **meist unwissentlich** in unberechtigte Hände und werden für kriminelle Zwecke weiterverarbeitet.

Diese moderne digitale Form von Betrug geschieht, besonders seit der fortschreitenden Digitalisierung während der Corona-Pandemie, per **E-Mail, SMS** oder mit **gefälschten Webseiten**.

Wie erkenne ich Phishing-E-Mails?

Besonders auffällig sind Nachrichten, welche Ihre Emotionen ansprechen, Angst oder Verbindlichkeit vermitteln und einen Zeitdruck hervorheben.

Hilfsbereitschaft:

E-Mails, die Mitgefühl, Mitleid und vermeintliches Liebesglück in den Mittelpunkt stellen sind ein beliebtes Mittel an sensible Daten zu gelangen. Versprechen, wie zum Beispiel ein Traumjob und eine Erbschaft oder Spendenaufrufe für Personen in Notlagen treten gehäuft auf.

Forderungen:

Nachrichten, welche mit Druck gefälschte Rechnungen bzw. Mahnungen für Waren oder Dienstleistungen einfordern, die Sie nie bestellt oder erhalten haben.

Vermeintliche Kontoaktualisierungen (DSGVO) und Verifizierungen.

Neugier:

Falsche Änderungen von Paketzustellungen: Aufforderung zum Öffnen des Dateianhangs oder Eingabe von Informationen in ein Formular.

Online-Übungen:

LearningApp: Phishing

LearningApp: Malware und Phishing

Phishing-Test: eBanking aber sicher!

ECDL: IT-Security

Medienberatung Weinviertel
Ing. Dr. Martin Lab, MSc BEd

M: 0664-88495717 | martin.lab@noemedia.at | www.noemedia.at

Wie kann ich mich und mein Kollegium schützen?

- ✓ Klicken Sie auf keine Links in E-Mails, in denen Sie dazu aufgefordert werden, Kontodaten oder Passwörter bekannt zu geben.
- ✓ Verschieben Sie diese E-Mails in Ihren Spam-Ordner.
- ✓ Informieren Sie die/den IT-Beauftragte/n Ihrer Schule.
- ✓ Übermitteln Sie keine vertraulichen Daten (Login-Daten, Passwörter, TANs etc.) per E-Mail, per Chat oder telefonisch.

Tipp:

Bewegen Sie Ihren Mauszeiger über den Absender oder einen Link ohne diesen anzuklicken. So können Sie überprüfen, ob der Name mit der E-Mail-Adresse oder Webseite in Verbindung steht.

Kann auch ich gefährliche E-Mails erhalten?

Ein klares **Ja!** Generell gilt:

- **!** Vorsicht vor Nachsicht.
- **!** Auf E-Mails mit fehlerhafter Rechtschreibung und Grammatik achten.
- **!** Verwenden Sie Ihre Dienst-Email-Adresse für Ihren Arbeitsalltag.
- **!** Öffnen Sie keine unbekannten Datei-Anhänge in E-Mails.
- **!** Antworten Sie nicht auf unbekannte E-Mails.
- **!** Überprüfen Sie, ob der Name des Absenders zur E-Mail-Adresse passt.

Weiterführende Inhalte und Quellen:

Fortbildungen der NÖ Media	Liste von aktuellen Phishing-E-Mails	Phishing-Radar: Aktuelle Warnungen
NÖ Media	Watchlist Internet	Verbraucherzentrale

https://sosafe.de/glossar/

https://www.saferinternet.at/

Medienberatung Weinviertel
Ing. Dr. Martin Lab, MSc BEd

M: 0664-88495717 | martin.lab@noemedia.at | www.noemedia.at