

eLearning - IT und ich: Mein Beitrag zur Sicherheit

IT-Seal ergänzt sein Awareness-Portfolio durch eLearning, welches anschaulich und verständlich Inhalte zum Thema Awareness vermitteln sollen. Aktuell (Stand: April 2019) steht ein WBT (=Web-based training) unter dem Titel "IT und ich: Mein Beitrag zur Sicherheit" zu Verfügung. Es umfasst fünf Module, die Dauer beträgt ca. 30 Minuten. Die WBT-Module liegen im SCORM-Format vor und können entweder auf Kunden- oder auf IT-Seal-Seite gehostet werden. Kunden können das WBT entweder als Gesamtpaket, oder einzelne Module kaufen.

eLearning wird im Rahmen vom Awareness Programm Lifetime oder eigenständig eingesetzt.

Das bisherige eLearning-Angebot umfasst die folgenden Themen-Bereiche. Weiter unten finden sich Screenshots für einen ersten Einblick.

WBT "IT und ich: Mein Beitrag zur Sicherheit"

Einführung: IT und ich

- Was sind Cyberangriffe? Wie werden Organisationen angegriffen? Wer greift an? "Es gibt doch Firewalls und Virens Scanner" - warum trage ich Verantwortung?

Social Engineering

- Erklärung: Was ist Social Engineering?
- Welche Tricks nutzen Angreifer?
- Wie läuft ein Angriff konkret ab?
- Wie schütze ich mich?

E-Mail-Sicherheit

- Was ist Phishing?
- Prominente Beispiele zu Datendiebstahl, Ransomware und CEO-Fraud
- Wie erkenne ich eine gefälschte E-Mail? Auf was sollte ich achten?
- Der Absender
- Wie erkenne ich das Ziel eines Links?
- Links lesen lernen
- Welche Dateianhänge sind gefährlich?

Soziale Medien: Risiken und Datenschutzeinstellungen

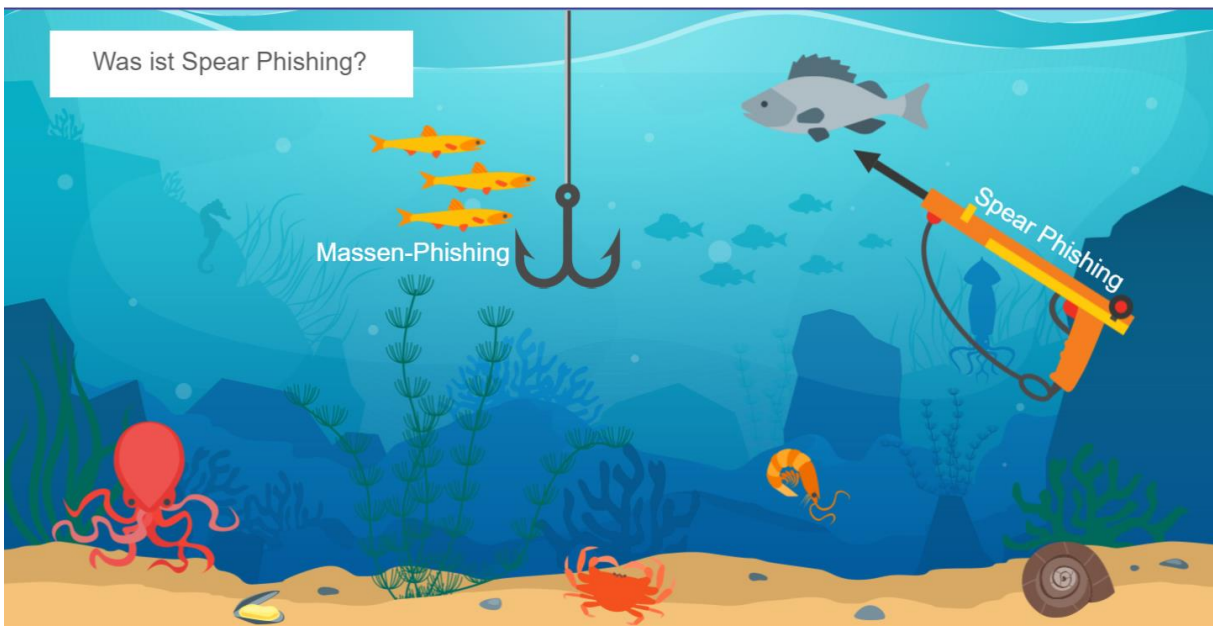
- Wieso bergen Soziale Medien eine Gefahr?
- Welche Informationen sind für Kriminelle interessant?
- Wie schütze ich mich? Datensparsamkeit, Datenschutzeinstellungen

Passwörter und Authentifizierung

- Warum sind starke Passwörter wichtig?
- Wie sieht ein sicheres Passwort aus?
- Wie verwalte ich Passwörter?
- Was bedeutet Zwei-Faktor-Authentifizierung?
- Tipps zur Erstellung eines sicheren Passworts



IT und ich: Einführung - IT als Teil unseres Lebens

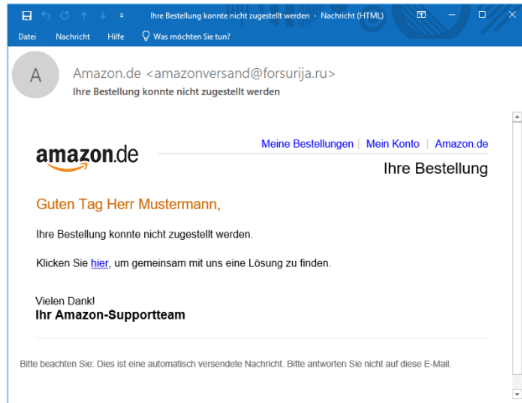


E-Mail-Sicherheit - Spear Phishing



Was denken Sie – ist die E-Mail echt oder gefälscht?

Klicken Sie auf das entsprechende Feld und bestätigen Sie Ihre Auswahl über den WEITER-Button.



Echt



Gefälscht



Schenken Sie der Absenderadresse einer E-Mail kein Vertrauen

Lassen Sie sich das Link-Ziel anzeigen

Prüfen Sie den Wer-Bereich:

<https://www.paypal.security-scanned.com/myaccount/transaction/details/8S716676K58992>

Achten Sie bei der Eingabe von Logindaten auf den Wer-Bereich in der Adresszeile

Vorsicht bei Dateianhängen, insbesondere .exe, .zip und .docm / .xlsm

Herzlichen Glückwunsch! Sie haben das Modul zum Thema E-Mail-Sicherheit erfolgreich abgeschlossen.

