Modul 4: Sicherheit

DiA – Digital in Arbeit

Bayerisches Staatsministerium für Familie, Arbeit und Soziales

DiA wird gefördert aus Mitteln des Arbeitsmarktfonds des Bayerischen Staatsministeriums für Arbeit, Familie und Soziales

f-bb Forschungsinstitut Betriebliche Bildung

Level 2

Lernziel:

Ergreifen von einfachen Maßnahmen zum Schutz des eigenen Gerätes und zum Energiesparen

Kapitel 2:
E-Mails: Schutz vor Spam und Phishing Mails

Spam

Unter Spam versteht man unerwünschte, meist massenhaft verschickte E-Mails.

Vergleichbar wie der heimische Briefkasten oft mit Werbung vollgestopft wird, wird auch der elektronische Briefkasten (also das E-Mail-Postfach) mit E-Mails zugemüllt, die Werbung oder unbestellte Nachrichten mit gefährlichem Inhalt enthalten. Doch anders als die Post im Briefkasten, die gefahrlos geöffnet werden kann, ist in der digitalen Welt Vorsicht geboten.

Spam-Mails können reine Werbung sein, aber auch Viren oder trojanische Pferde enthalten oder Phishing-Mails sein.

Arten von Spam

Es gibt verschiedene Arten von Spam:

- **Werbung**: Nervig, aber ungefährlich

- **Virus oder Trojanisches Pferd**: die absendenden Personen der E-Mail wollen Sie dazu bringen, einen mitgelieferten Datei-Anhang – oft im zip-Format - zu öffnen. In diesem ist ein Schadprogramm enthalten, beispielsweise ein Virus, d.h. ein sich selbst verbreitendes Computerstörprogramm. Oder ein trojanisches Pferd, ein Programm, das – ist es erst installiert – den Kriminellen Zugang zum Computer verschafft.

- **Geldversprechen**: In den E-Mails wird z.B. eine reiche Erbschaft oder die Möglichkeit versprochen, mit wenig Arbeit viel Geld zu verdienen. Hier geht es den Kriminellen um Ihre persönlichen Daten und dann ihr Geld oder sogar um illegale Geldwäsche oder sonstige illegale Geschäfte.

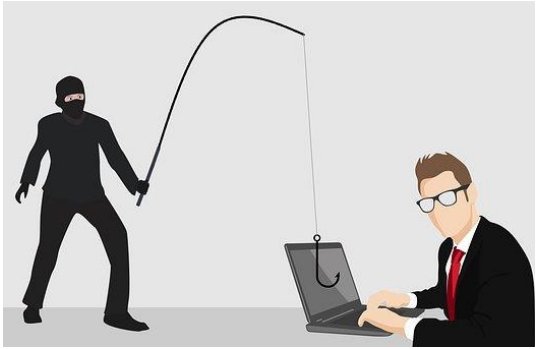
- **Hoax**: eine Falschmeldung, die von vielen für wahr gehalten und daher an Freunde/Freundinnen, Kolleg*innen, Verwandte und andere Personen weitergeleitet wird.

Verbraucherzentrale: Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf

Phishing

„Phishing ist ein Kunstwort aus "Passwort" und "Fishing" und bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden.“

Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de)



Den Kriminellen geht es also darum, Sie dazu zu bringen, persönliche Daten wie beispielsweise PIN, Girokontonummer oder Kreditkartennummer preiszugeben.

Verbraucherzentrale: Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf

Phishing-Mails

Die Phishing-E-Mail wird dazu so konstruiert, dass sie Vertrauen schafft und den Eindruck erweckt, von einem echten Anbieter zu stammen.

Meistens arbeiten die Kriminellen mit einem Link, der Sie zu einer Seite mit einer Eingabemaske für persönliche Daten führt.

Oder Sie werden dazu aufgefordert, einen Datei-Anhang zu öffnen. Dieser enthält dann ein Schadprogramm wie ein trojanisches Pferd, mit dem die Kriminellen sich Zugang zu Ihrem Computer verschaffen.

Aufbau von Phishing-Mails

1. **Anrede:** oft allgemein (z.B. „Sehr geehrter Kunde“), immer öfter aber auch persönlich mit Vor- und Nachnamen

2. **Grund der E-Mail:** Beliebt sind zum Beispiel Gesetzesänderungen, die Einführung einer neuen Sicherheitstechnik oder Unstimmigkeiten im Kundenkonto, die geklärt werden müssen.

3. **Notwendigkeit zum Handeln:** E-Mail-Empfänger*in soll aktiv werden. In der Regel soll er seine/sie ihre Daten erneut eingeben, kontrollieren, bestätigen oder verifizieren.

4. **Zeitdruck:** Damit die E-Mail-Empfänger*innen nicht zu lange nachdenken können und am Ende doch noch misstrauisch werden, gibt es nur eine kurze Zeitspanne für das vermeintlich notwendige Handeln.

5. **Konsequenzen des Nichthandelns:** Wer nicht innerhalb dieser kurzen Frist aktiv wird, dem werden schwere Konsequenzen angedroht. Oft geht es darum, dass ein Konto eingeschränkt wird, gar nicht mehr genutzt werden kann oder sogar aufgelöst wird.

6. **Link oder Anhang:** Die Kriminellen fügen der E-Mail einen Link oder einen Datei-Anhang bei, der geklickt bzw. geöffnet werden soll, um das Problem ganz einfach zu lösen. Ganz selten wird eine Antwort per E-Mail erbeten.

Verbraucherzentrale: Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf

Wie erkenne ich Phishing-Mails?

Eines oder mehrere der folgenden Kriterien deuten auf eine Phishing-Mail hin:

- Eine **allgemeine Anrede** wie „Liebe Kunden“ oder „Sehr geehrte Damen und Herren“.
- Die E-Mail ist **nicht auf Deutsch**, sondern z.B. auf Englisch verfasst. Ein deutscher Anbieter würde Sie nicht auf Englisch anschreiben.
- Die E-Mail wurde **mit Hilfe eines Computerprogramms ins Deutsche übersetzt**, erkennbar z.B. an einer Reihe von Tippfehlern, von der falschen Darstellung von z.B. ß, von Sätzen, die keinen Sinn ergeben und von einzelnen Wörtern, die gar nicht übersetzt wurden. Eine solche E-Mail würde ein echter deutscher Anbieter nie verschicken.

Wie erkenne ich Phishing-Mails?

Es gibt aber auch Phishing-E-Mails, die professionell gestaltet sind, die nicht die genannten Merkmale aufweisen und daher deutlich gefährlicher sind. Es gibt eine **persönliche** Anrede und **keine** grammatikalischen Fehler.

Aber auch bei diesen gibt es Kriterien, die auf einen Betrugsversuch hindeuten:

- Wenn Sie tatsächlich Kunde oder Kundin bei diesem Unternehmen sind, dieser Anbieter Sie aber sonst nicht per E-Mail kontaktiert, ist die Wahrscheinlichkeit besonders hoch, dass die E-Mail nicht echt ist. Wenn Sie bei diesem Anbieter gar nicht Kunde/Kundin sind, gilt dies erst recht.

- Sie finden den oben beschriebenen Aufbau von Phishing-Mails vollständig oder zumindest weitgehend wieder.
- Die Absenderadresse ist gefälscht. Die Adresse, die zu sehen ist, stimmt nicht mit der Adresse überein, die im Header steht. (Hinweis: Was der Header ist und wie Sie diesen einsehen können, erläutert die Verbraucherzentrale auf www.vz-nrw.de/phishing)
- Die Internetadresse, die im Text angegeben ist, stimmt nicht mit der Internetadresse überein, zu der der Link tatsächlich führt. Dies können Sie leicht herausfinden: Gehen Sie mit der Maus auf den Link, ohne auf diesen zu klicken – auf dem Bildschirm wird angezeigt, wo der Link tatsächlich hinführt.

Verbraucherzentrale: Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf

Umgang mit Spam-Mails

Die drei wichtigsten Regeln im Umgang mit unerwarteten Mails lauten:

- Klicken Sie niemals auf Links.
- Öffnen Sie niemals Datei-Anhänge.
- Antworten Sie nicht auf diese Mails

Wenn Sie diese drei Regeln beherzigen, haben Sie die größte Gefahrenquelle im Umgang mit unerwarteten E-Mails schon ausgeschaltet.
Haben Sie eine Mail als Betrugsversuch entlarvt, löschen Sie diese.

Verbraucherzentrale: Phishing_und_trojanische_Pferde_Angriffe_auf_den_eigenen_PC_erkennen_und_abwehren.pdf

Übung 1

Spam, Phishing, Hoax –
Können Sie richtig zuordnen?

Hier geht’s zur Übung

Übung 2

Handelt es sich um Phishing oder um echte E-Mails? Können Sie es erkennen?

Hier geht’s zur Übung

Viel Erfolg beim Ausprobieren!

Bayerisches Staatsministerium für Familie, Arbeit und Soziales

DiA wird gefördert aus Mitteln des Arbeitsmarktfonds des Bayerischen Staatsministeriums für Arbeit, Familie und Soziales

f-bb Forschungsinstitut Betriebliche Bildung