



Phishing Mails

4

E-Mail II
Erwachsene

4

E-Mail II

Phishing Mails

Präsentation Folie 2

Jetzt reden wir über das Thema Phishing Mails.

Weiß jemand von euch, was das ist?

Ich nehme die Wortmeldungen dran.

Wenn es keine Wortmeldungen mehr gibt, mache ich weiter.

Nächste Folie

Präsentation Folie 3

Bei **Phishing Mails** werden Daten **gestohlen**.

Genauer gesagt: Eine Person will deine persönlichen Daten bekommen.

Zum Beispiel: Das Passwort zu einem Online-Shop oder zu eurem Online-Banking.

Dafür schauen wir jetzt gemeinsam einen kurzen Film an.

Nächste Folie

Präsentation Folie 4

Ich klicke auf den Link in der Präsentation und klicke rechts unten im Videofenster auf das Vollbild-Symbol.

Nach dem Video klicke ich wieder auf das Vollbild-Symbol und gehe zurück in die Präsentation.

Nächste Folie

Präsentation Folie 5

Hier seht ihr eine **Liste**, wie wir Phishing Mails erkennen.

Erstens: Wir sollten immer den Absender überprüfen.

Oft nutzen Phishing Mails zum Beispiel den Namen von Freunden oder Firmen, die wir kennen.

Deshalb sollten wir die E-Mail-Adresse des Absenders genau anschauen.

Präsentation Folie 5

Zweitens: Achtung bei Links.

Links können uns auf eine gefälschte Internetseite bringen.

Dort werden dann zum Beispiel unsere Passwörter abgefragt.

Selbst wenn ihr den Absender kennt: Macht euch Gedanken, ob die Mail für euch Sinn ergibt.

Und überprüft, ob verlinkte Internetseiten vertrauenswürdig sind.

Präsentation Folie 5

Drittens: Das ist auch wichtig für E-Mail-Anhänge.

Bekommt ihr einen E-Mail-Anhang, der komisch ist?

Im Text und Betreff der E-Mail wurde kein Anhang erwähnt?

Oder endet die Datei mit .exe oder .msi?

Dann öffnet den Anhang nicht und überprüft den Absender der E-Mail.

Präsentation Folie 5

Viertens: Ihr solltet niemals sensible Daten in einer E-Mail verschicken.

Damit meine ich zum Beispiel Passwörter oder Kontodaten.

Keine echte Firma wird euch danach fragen.

Wenn ihr eine solche Anfrage per E-Mail bekommt, ist das eine Phishing-Mail.

Präsentation Folie 5

Fünftens: Achtet auf die Sprache in E-Mails, die ihr bekommt.

Sind in einer E-Mail von eurem Telefonanbieter zum Beispiel viele Rechtschreibfehler, dann ist das wahrscheinlich eine Phishing Mail.

Ein weiterer Hinweis könnte sein: Ihr werdet unpersönlich angesprochen.

Zum Beispiel: „Lieber Kunde, ...“ oder nur „Guten Tag, ...“

Präsentation Folie 5

Dann überprüft bitte den Absender genau.

Sechstens: Lasst euch nicht unter Druck setzen!
Und nehmt euch Zeit!

In vielen Phishing Mails steht, dass ihr schnell antworten müsst, weil sonst ein Konto von euch gesperrt wird.

Oder etwas anderes gefährliches passiert.

Auch das wird eine echte Firma euch niemals schreiben.

Präsentation Folie 5

Ihr müsst keine Angst bekommen, wenn so etwas in einer E-Mail steht.

Und klickt natürlich auch in solchen Mails nicht auf Links!

Nächste Folie

Präsentation Folie 6

Diese sechs Tipps könnt ihr euch auf diesem **Bild** noch einmal in Ruhe anschauen.

Ihr bekommt nach dieser Einheit eine **Liste** mit einem QR-Code zu dieser Übersicht.

Nächste Folie

Präsentation Folie 7

Jetzt habe ich eine **Frage an euch**:

Habt ihr schon Phishing Mails bekommen?

Was stand darin?

Habt ihr vielleicht eine Phishing-Mail auf eurem Smartphone dabei?

Ich nehme die Wortmeldungen dran.

Wenn es keine Wortmeldungen mehr gibt, mache ich weiter.

Nächste Folie

Präsentation Folie 8

Aber was machen wir, wenn wir eine Phishing Mail zu **spät erkennen**?

Wir haben vielleicht schon unsere persönlichen Daten auf einer gefälschten Internetseite eingegeben.

Zum Beispiel dein Passwort für dein Online Banking.

Als erstes sollte ich die Bank informieren, dass jemand anderes wahrscheinlich meine Zugangsdaten hat.

Präsentation Folie 8

Die Bank wird mir dann auch sagen, was ich noch tun kann.

Ich sollte dann sofort das Passwort bei meiner Bank ändern.

Nächste Folie

Präsentation Folie 9

Unter diesem Link findet ihr weitere Informationen dazu.

Ich öffne den Link und zeige die beiden Seiten der Checkliste.

Auf diesen beiden Seiten findet ihr weitere Tipps zu Phishing Mails.

Ihr bekommt diesen Link als QR-Code später noch von mir.

Ich wechsle wieder zur Präsentation zurück.