



Phishing Mails

4

E-Mail II
Erwachsene

Was sind Phishing-Mails?



Phishing Mails = Datendiebstahl



Video: Phishing

https://multimedia.gsb.bund.de/BSI/Video/Sicher_im_Internet/Phishing.mp4

Phishing E-Mails erkennen

1. Absender prüfen!
2. Vorsicht bei Links!
3. Dateianhänge prüfen!
4. Keine sensiblen Daten weitergeben!
5. Auf die Sprache achten!
6. Nicht unter Druck setzen lassen!
Nimm dir Zeit!

Vorsicht, Phishing! Betrügerische E-Mails erkennen

1. Absender prüfen – ist die E-Mail echt?

Schaut genau auf die Absenderadresse, bevor ihr auf eine E-Mail reagiert. Falls euch die Adresse merkwürdig vorkommt, ruft den Absender persönlich an oder schreibt ihm über einen bekannten Kommunikationsweg, um die Echtheit zu überprüfen.

2. Vorsicht bei Links!

Enthält die E-Mail eine Verlinkung zu einer anderen Webseite? Wird bei einem Mouseover eine verdächtige oder unbekannte Webadresse angezeigt, dann könnte sich dahinter ein Phishing-Versuch verbergen.

3. Dateianhänge? Nein, danke!

Achtung bei E-Mails mit Dateianhängen! Dateiendungen wie .exe, .zip, .xls, .iso, .docx oder kryptische Formate werden von Kriminellen gerne verwendet, um darin Schadsoftware zu verstecken.

4. Keine sensiblen Daten weitergeben!

Unternehmen oder Behörden fragen nie per E-Mail nach Passwörtern, Bankdaten oder anderen vertraulichen Informationen. Wenn ihr persönliche Daten eingeben sollt, seid misstrauisch und fragt über offizielle Wege bei der anschreibenden Organisation nach.

5. Achtet auf die Sprache!

Große Unternehmen und bekannte Organisationen legen viel Wert auf korrekte Sprache – eine schlecht geschriebene Nachricht oder eine unpersönliche Anrede („Sehr geehrter Kunde“ statt eures Namens) ist ein Anzeichen für eine betrügerische E-Mail.

6. Lasst euch nicht unter Druck setzen!

Phishing-Mails versuchen oft, Panik zu erzeugen: „Ihr Konto wird gesperrt!“ oder „Handeln Sie sofort, sonst...“. Bleibt ruhig und überlegt, ob ihr diese Nachricht überhaupt erwartet habt.



© Bundesamt für Sicherheit in der Informationstechnik | Bildnachweis: AdobeStock©Phruetthiphong

Welche Phishing-Mails habt ihr bekommen?



Was soll ich tun?

1. Bank informieren
2. Neues Passwort anlegen



Was soll ich tun?

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser Checklisten Flyer/Checkliste BSI ProPK Phishing.pdf? blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser%20Checklisten%20Flyer/Checkliste%20BSI%20ProPK%20Phishing.pdf?__blob=publicationFile&v=5)