**Infoblatt „Spam und Phishing“**

**Gefahren bei der Verwendung von E-Mail-Diensten**

**Welche Gefahren und Risiken begegnen Ihnen als Nutzer\*in von E-Mail-Diensten?**

E-Mail ist der am meisten genutzte Internetdienst und deshalb die ideale Plattform für Betrug. Nachfolgend sind einige der Gefahren aufgelistet, mit denen Sie als Nutzer\*in konfrontiert sein können:

* Spam (Junk)
* Phishing
* Schadsoftware (z. B. Viren, Würmer, Trojaner ...)
* missbräuchliche Nutzung des E-Mail-Kontos

****

**1. Spam-Mails**

Unter Spam-Mails versteht man unerwünschte E-Mail-Nachrichten, die massenhaft verschickt werden. Ziel solcher E-Mails ist, dass Sie ein Produkt kaufen oder eine Website bzw. einen E-Mail-Anhang öffnen. In letzterem kann sich eine Schadsoftware (z. B. ein Computer-Virus) verstecken.

**Woran erkennen Sie Spam-Mails? Welche Hinweise deuten auf Spam-Mails?**

1. **Rechtschreibung und Grammatik**

Bei E-Mails, die viele Rechtschreib- oder Grammatikfehler beinhalten, handelt es sich oft um Spam-Mails. Diese werden nämlich oft mithilfe von Apps übersetzt.

1. **Fremdsprachige E-Mails**

Finden Sie plötzlich eine E-Mail in einer Fremdsprache (z. B. Englisch oder Russisch) in Ihrem Posteingang, könnte dies auch ein Anzeichen für Spam sein.

1. **Falsche Versprechungen**

Oft werden Ihnen hohe Gewinne versprochen oder Produkte kostenlos oder extrem günstig angeboten.

1. **Unpassende Anrede**

Einen Hinweis liefert auch der Blick auf die Ansprache. Wenn Sie nicht mit Ihrem Nachnamen angesprochen werden, ist die E-Mail meist nicht seriös. Es ist auch nicht seriös, wenn Sie von Unbekannten in einem sehr vertraulichen Ton angesprochen werden („Meine Liebe“…).

1. **Unbekannte Absender\*innen**

Prüfen Sie immer genau, ob Sie die/den Absender\*in kennen oder ob Ihnen das Unternehmen bekannt vorkommt.

1. **Anhänge (Attachments)**

Grundsätzlich sollten Sie niemals den Anhang einer potentiellen Spam-Mail öffnen. Oft sieht die Schadsoftware auf den ersten Blick wie ein harmloses Dokument aus.

Gefährliche Dateianhänge tragen häufig diese Endungen:
 .exe, .com, .pif oder .scr

**2. Phishing-Mails**

Phishing wird der Trick genannt, geheime Daten herauszulocken. Solche Daten sind z. B.

* Passwörter
* Zugangsdaten für das Online-Banking
* Kontodaten
* Kreditkartendaten
* persönliche Informationen
* …

Ein Phishing-Mail kann ein **verlockendes Angebot** enthalten oder Sie unter einem Vorwand unter **Druck** setzen,

* damit Sie ein gefälschtes Formular ausfüllen,
* den Link zu einer gefälschten Webseite anklicken oder
* einen E-Mail-Anhang mit einer Schadsoftware (z. B. einem Computervirus) öffnen.

Aber: Ihre Bank würde Sie niemals per E-Mail auffordern, auf einer anderen Webseite Ihre Zugangsdaten einzugeben!

Ansonsten gelten dieselben Erkennungszeichen für Phishing-Mails wie bei Spam-Mails – siehe vorige Seiten.

**3. Wie können Sie sich bei der Nutzung von E-Mail vor Gefahren schützen und Ihr Risiko minimieren?**

Es gibt kein Patentrezept oder 100%igen Schutz, aber mit einigen Verhaltensregeln können Sie die E-Mail-Gefahren sehr minimieren:

* die eigene E-Mail-Adresse nicht im Internet veröffentlichen
* E-Mail-Adresse so wenig wie möglich auf Webseiten verwenden
* sichere Passwörter für alle Online-Dienste verwenden
* mehrere E-Mail-Adressen verwenden
* auf Spamfilter und Virenschutz achten
* u. v. m.

TIPP:

Wenn Sie sich nicht sicher sind, ob die E-Mail nicht doch wichtig ist, suchen Sie im Internet nach dem Namen und der E-Mail-Adresse des/der Absender\*in oder nach dem E-Mail-Betreff. Es gibt Webseiten, auf denen Spam-Mails und Phishing-Mails gesammelt werden. So können Sie sich schnell Klarheit verschaffen!

Weitere Informationen und Beispiele für Spam- und Phishing-Mails finden Sie in der Datei: Unterlagen\_spam-und-phishing.pdf