

## Tipps gegen Cyberkriminalität und Phishing.

Wir haben hier ein paar wichtige Tipps für Sie zusammengestellt:

**E-Mail-Absender prüfen.** Ist die Absenderadresse bekannt? Handelt es sich um einen vertrauenswürdigen Absender? **Doch Vorsicht.** Auch bekannte oder vertrauenswürdige (echte) Adressen können bereits „gehackt“ worden sein! Im Zweifel besser den „vermeintlichen“ Absender auf einem anderen Kommunikationsweg (z.B. Telefon) kontaktieren und nachfragen.



Aktuell unterstützt auch bereits die „KI“ (künstliche Intelligenz) die Kriminellen bei der Erstellung von E-Mails, die dann „seriös“ und echt wirken. So sind das „Layout“ und auch die Sprache, die vormals häufig auf „Fake-E-Mails hindeuteten heute nicht mehr unbedingt entscheidend.

**Vorsicht bei „links“.** Da „links“ so ungemein praktisch sind, werden diese auch gerne von Kriminellen eingesetzt um uns zu überlisten. **Hier lauert Phishing.** Auch hierzu sollte ggf. nachgefragt werden, ob der angezeigte und grundsätzlich vertrauenswürdige Absender den „link“ tatsächlich versendet hat. Auch bei bekannten großen Dienstleistern und Zustellservices kann Vorsicht geboten sein. Die Praxis ist, dass E-Mails mit „links“ zum Sendungsstatus versendet werden... Doch ist die E-Mail und der „link“ auch echt?

**Zusatz-Tipp:** Um sicher zu gehen, kann auch auf der offiziellen Homepage meist eine direkte „Sendungsverfolgung“ abgerufen werden. Unter Eingabe der „Sendungsnummer“ erhalten wir ebenso Auskunft und das ganz ohne das Risiko eines ggf. gefakten „links“.

**Passwörter und Zugangsdaten niemals mitteilen.** Geben Sie niemals am Telefon, per SMS, WhatsApp, E-Mail usw. Kennwörter oder Zugangsdaten bekannt. Seien Sie von vornherein skeptisch, wenn jemand danach fragt. Behörden, Banken und Sparkassen würden Sie niemals danach befragen.

**Banking besser nicht via Smartphone.** Die 2-Faktoren-Authentifizierung ist ohnehin ein Muss! Die strikte Trennung des Zugriffs auf die Banking-Anwendung der Bank/Sparkasse und der 2-Faktoren-Authentifizierung sollte strikt eingehalten werden. Keine Bankgeschäfte über das Smartphone.

## Tipps gegen Cyberkriminalität und Phishing.

**Vorsicht bei öffentlichem W-LAN / WiFi.** Ein Internetzugang über frei zugängliche W-LAN-Netzwerke sollte –wenn überhaupt– mit Zurückhaltung und Vorsicht genutzt werden. Hacker haben hier quasi freie Bahn um Ihren „Geschäften“ nachzugehen.

**Immer aktuelle Sicherheitssoftware (Virenschutz-Software) einsetzen.** Stets regelmäßige Updates wahrnehmen.

Hierzu eine Veröffentlichung vom BSI (Bundesamt für Sicherheit in der Informationstechnik)

### 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

### FAZIT:

**Seien Sie vorsichtig. Handeln Sie mit Bedacht.**

**Ein schneller „Klick“ in Eile und es ist passiert.**