Checkliste

Finanzbetrug

Woran kann man Finanzbetrug erkennen?

✓		Folgende Schritte sind zu setzen:
☐	**Achte auf Warnsignale!**	Es kommt vor, dass wir nicht besonders aufmerksam sind, wenn wir unsere E-Mails abrufen, digitale Nachrichten erhalten oder im Internet surfen. Diese Unaufmerksamkeit nutzen Kriminelle. Deshalb sollten wir auf Warnsignale achten, die einen Betrug enttarnen können und die hier beschrieben sind. Beachte bitte: Unternehmen und Banken fragen niemals nach vertraulichen Daten wie Passwörtern und Zugangsdaten per E-Mail, SMS oder Telefon!
☐	**Unpersönliche Anrede**	Eine unpersönliche E-Mail-Anrede, in der Empfängerinnen und Empfänger mit „Hallo“ oder „Sehr geehrter Benutzer“ angesprochen werden, kann ein erster Hinweis auf einen Phishing- oder Scam-Versuch sein.
☐	**E-Mail-Adresse des Absenders/der Absenderin**	Kriminelle verwenden E-Mail-Adressen, die nicht mit den E-Mail-Adressen des Unternehmens oder der Institution übereinstimmen. Diese können aber sehr ähnlich zu den echten E-Mail Adressen sein. Oft wird am Anfang der Mailadresse der Name eines bekannten Unternehmens verwendet, damit man denkt, dass das Unternehmen der Absender ist. Hinterlegt ist aber die betrügerische Zielseite.
☐	**Dringlichkeit der Nachricht**	Phishing- und Scam-Nachrichten drängen Empfängerinnen und Empfänger dazu, rasch zu handeln, um weiteren Schaden wie die Sperre des Kontos oder die Kündigung des Vertrags (beispielsweise bei Online-Streaming-Plattformen) zu vermeiden oder eine gewinnbringende Gelegenheit nicht zu verpassen. Der Zeitdruck soll dazu führen, dass Links unüberlegt angeklickt und Informationen weitergegeben werden.

☐	**Links zu verdächtigen Seiten**	Links in Nachrichten und E-Mails können zu betrügerischen Seiten oder Schadsoftware führen und sollten deswegen prinzipiell nicht angeklickt werden. Überlege genau, ob du weißt, woher die Nachricht stammt. Bei Unsicherheit kann man sich wie gewohnt beim Anbieter anmelden (in der App oder über die Web-Adresse) und dort überprüfen, ob es Handlungsbedarf gibt. Bei Verdacht auf Missbrauch sollte man das Passwort des betroffenen Accounts sofort ändern. Verdächtige Seiten kannst du außerdem über das Meldeformular der watchlist-internet.at melden.
☐	**Verdächtige Dateianhänge**	Ungewöhnliche Dateianhänge enthalten oftmals Schadsoftware, die sich auf dem Gerät installiert und sensible Daten an Kriminelle weiterleitet.
☐	**Rechtschreib- und Grammatikfehler**	E-Mails von Betrügerinnen und Betrügern enthalten oftmals Rechtschreib- und Grammatikfehler. Manchmal ist auch der ganze Text eine schlechte Übersetzung aus einer anderen Sprache.
☐	**Fehlende Informationen zum Unternehmen**	Bei unseriösen Online-Shops fehlen häufig das Impressum, Hinweise auf Rechte von Konsumentinnen und Konsumenten sowie Kontaktmöglichkeiten des Unternehmens.
☐	**Sperren von Mehrwertnummern**	Du kannst deine Nummer für Mehrwertdienste sperren lassen. Oft reicht dazu die App deines Mobilfunkanbieters, in der du die Sperre selbst vornehmen kannst oder ein Anruf bei der Serviceline. So kannst du vermeiden, dass unerwünschte Abbuchungen entstehen.