ACHTUNG BETRUGSVERSUCHE!

Es gelingt Betrügern immer wieder mit Telefontricks oder im Internet Menschen um ihr Erspartes zu bringen.
Ich möchte hier weiters einige der bekannten Tricks auflisten, leider kann diese Liste nicht vollständig sein, da sich die Betrüger immer neue Betrugsmaschen einfallen lassen. Mittels Künstlicher Intelligenz werden die Tricks immer „realitätsangepasster".

Bestellbetrug

Die Täter geben sich entweder als Besteller oder als Verkäufer aus. Betrüger können z.B. mit gestohlenen Identitäten Waren bestellen, ohne diese zu bezahlen. Die Mahnungen gehen dann an jene Personen, deren Daten widerrechtlich verwendet wurden. Andererseits stellen sich Betrüger auf Kleinanzeigen und Plattformen als seriöse Anbieter dar. Nach Vorauszahlung der angebotenen Waren werden diese jedoch nicht versandt. Fake-Shops wirken oft wie seriöse Plattformen, entpuppen sich jedoch als Betrugsfalle. Die Geschädigten erhalten keine oder minderwertige Ware. Die angeblichen Verkäufer sind auch nicht mehr erreichbar. Daher überprüfen Sie die Seriosität der Anzeiger; beachten Sie Kundenrezessionen; überlegen Sie, ob der Preis realistisch ist oder ob das Angebot „zu schön ist, um wahr zu sein". Seriöse Onlineshops und Kleinanzeigen-Plattformen haben ein Impressum und die Verantwortlichen reagieren auf Anfragen.

Phishing

Täter versuchen persönliche Daten über das Internet zu erlangen. Via Mails oder betrügerischen Websites werden persönliche Daten oder Informationen wie Kreditkartennummern, Kontodaten sowie Zugangsdaten zu Ihren E-Mail- und anderen Accounts abgefragt. Fingierte E-Mails sollen z.B. beim Adressaten den Eindruck erwecken, sie kämen von einer Bank. Es wird gefordert, man solle einen Link anklicken, von dem man zu einer meist täuschend echt aussehenden Betrugs-Website geleitet wird. Das Opfer wird unter einem Vorwand gebeten, seine persönlichen Daten, darunter auch Passwörter, Pins und Tans, einzutragen. Im Schadensfall nehmen Sie bitte sofort mit dem betroffenen Dienstleister (Bankinstitut, Paypal, Ebay, Amazon, etc. Kontakt auf, informieren diesen vom Vorfall und veranlassen die sofortige Sperre. Danach erstatten Sie umgehend Anzeige auf einer Polizeiinspektion!

Betrügerische Investment-Seiten im Internet

Potenzielle Anleger werden im Internet zu Geldzahlungen für vermeintlich lukrative Investitionsgeschäfte verleitet. Die Oper werden über Internet-Werbeanzeigen, soziale Netzwerke, Anrufe aus eigens geschaffenen Call-Centern oder Mas-

senmails angeworben. Es werden anfangs hohe Gewinne vorgetäuscht, um die Opfer zu weiteren Zahlungen zu verleiten. Das bezahlte Geld wird nicht angelegt, sondern verschwindet im kriminellen Netzwerk!

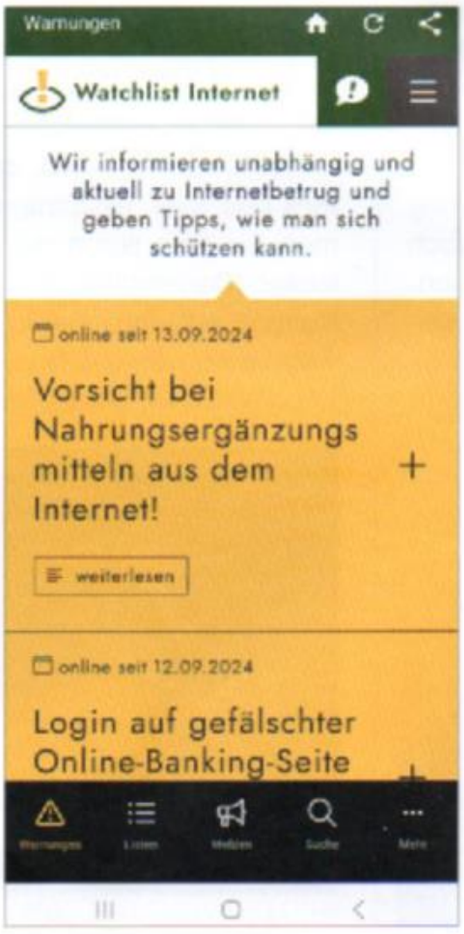
Tipps:

Aktualisieren Sie laufend Ihre Software, halten Sie Ihr Betriebssystem, Ihre Apss und Ihren Virenschutz auf dem neuesten Stand. Aktualisierte Software enthält oft Sicherheitsverbesserungen.

Verwenden Sie sichere Zahlungsmethoden wie Kreditkarten oder PayPal. Diese bieten oft zusätzlichen Schutz in Falle von Betrug.

Melden Sie verdächtige Aktivitäten, wenn Sie verdächtige E-Mails, Anrufe oder Websites bemerken, melden Sie diese an die entsprechenden Behörden oder Plattformen.

Laden Sie sich die **App Watchlist AT auf Ihr Gerät.** Sie werden von amtlicher Seite unabhängig und aktuell zu Internetbetrug informiert und bekommen Tipps, wie man sich schützen kann. Unseriöse Webseiten können gemeldet werden, „verdächtige Webseiten" können überprüft werden.



Lassen Sie sich nicht unter Druck setzen, erfragen Sie Details, die nur der richtige Verwandte oder Bekannte, welche angeblich anruft, wissen kann. Meldet sich der Anrufer nicht selbst, fragen Sie nach dem Namen, raten Sie nicht, wer anruft, sondern fordern Sie den Anrufer dazu auf, sich selbst zu identifizieren!

Geben Sie **am Telefon nie vertrauliche Informationen preis.**

Kein seriöses Unternehmen oder Bankinstitut fordert per Mail zur Eingabe persönlicher Daten wie Passwörter auf. Überprüfen Sie die Adresszeile des Webbrowsers. Wichtige Homepages, wie z.B. Bankzugang, können als Favoriten im Browser eingerichtet und nur dieser Zugang verwendet werden. Niemals ein Passwort für mehrere Dienste! Das Passwort sollte mindestens 8 Zeichen lang sein, aus einer Reihe von Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. **Kreditkarten- und Bankinstitute sowie Online-Shops fordern niemals per E-Mail zur Bekanntgebe von Daten auf!**

Nehmen Sie **keine Anrufe mit unterdrückter Nummer entgegen.**

Rufen Sie nie bei einem verpassten Anruf mit einer Ihnen unbekannten Nummer zurück. Der Anrufer wird sich wieder melden, wenn es ihm wichtig ist. Achten Sie darauf, welche Vorwahl die Nummer hat, um Kosten zu vermeiden.

Geben Sie **kein Geld oder Wertsachen** wie Schmuck **an unbekannte Personen**, auch nicht an die „Polizei".

Es werden immer neue Methoden von Betrügern entwickelt, um Menschen zu täuschen. Bleiben Sie wachsam und hinterfragen die Plausibilität z.B. des Anrufes, der E-Mail, etc.!

Hauptquelle:
www.bundeskriminalamt.at

Mag. Luise Gerstendorfer