Digitale Sicherheit 4/6

PHISHING, SPAM & BETRUG ERKENNEN – UND RICHTIG REAGIEREN

Worum geht's?

Gefälschte Mails, betrügerische SMS und dubiose Anrufe sind inzwischen Teil des digitalen Alltags. Sie wirken oft täuschend echt – mit dem Ziel, an Passwörter, Kreditkartendaten oder andere persönliche Informationen zu gelangen. Dieses Infoblatt zeigt, wie du solche Betrugsversuche erkennst und dich davor schützt.

Kennst du diese Betrugsmaschen?

Eine Mail „von deiner Bank" fordert dich auf, deine Daten zu aktualisieren

Eine SMS mit Paketankündigung enthält einen merkwürdigen Link

Eine Gewinnbenachrichtigung verlangt „nur kurz" deine Kartennummer

Ein Anrufer gibt sich als Polizist aus.

4 Dinge, die du sofort umsetzen kannst

1. Links & Anhänge immer hinterfragen:
Keine Daten eingeben oder Dateien öffnen, wenn du den Absender nicht klar erkennst. Im Zweifel: direkt bei der Firma nachfragen – aber nie über den Link in der Mail!

2. Verdächtige Nachrichten löschen oder melden:
Spam und Phishing gehören sofort gelöscht. Viele Mailprogramme oder SMS-Apps bieten auch eine „Melden"-Funktion..

3. Keine Daten am Telefon weitergeben:
Keine Bank, kein Tech-Unternehmen und keine Behörde fragt telefonisch nach Passwörtern oder Codes. Einfach auflegen – das ist erlaubt!

4. Zwei-Faktor-Authentifizierung aktivieren:
Wenn Betrüger doch an ein Passwort kommen, schützt ein zusätzlicher Code (z.B. per SMS oder App) vor dem Zugriff auf dein Konto.

Hör-Tipp: SRF Espresso

Willst du mehr wissen?

Tipps zu Internetbetrug: **https://www.ibarry.ch.**
Aktuelle Betrugsmaschen: **https://cybercrimepolice.ch**
YouTube-Tipp: **Phishing-E-Mails enttarnen!**

Was kommt als Nächstes?

Im Oktober geht's um Künstliche Intelligenz (KI) und Deepfakes was steckt dahinter und wo lauern Gefahren.
Wenn du Fragen hast oder dir ein Thema besonders wichtig ist – meld dich einfach bei Emanuel Petrig.
Petrig@outlook.com

RURACTIVE Törbel-Moosalpregion