

BETRUG IN SOZIALEN NETZWERKEN

Nirgendwo sonst findet Internet-Betrug so geballt statt wie bei **Facebook & Co.** Der fatale Klick auf einen **vierversprechenden Link oder Werbebanner** ist schnell passiert. Die versprochenen Inhalte gibt es nicht, dafür allerhand Probleme: unwissentlich abgeschlossene **Abos**, die **Weitergabe persönlicher Daten** an Adresshändler, **Computerviren**, ein **gehacktes Profil** usw. Auch ein Risiko: „**Falsche**“ **Freunde**, die via Chat um Geldtransfers oder Anrufe bei teuren Telefonnummern bitten. Vorsicht auch bei schockierenden Videos: Dahinter stecken teure Abofallen, das Video gibt es gar nicht.

TIPPS

- Nicht unüberlegt auf allzu verlockend klingende Links in Postings, Nachrichten oder Werbeanzeigen klicken. Auch nicht, wenn die „Empfehlung“ scheinbar von Freunden kommt.
- Skeptisch sein, wenn von Personen eine Freundschaftsanfrage kommt, die eigentlich schon in der Kontaktliste sind.
- Immer genau lesen, was mit dem Absenden eines Formulars oder der Bestätigung per Klick akzeptiert wird (Kleingedrucktes!).
- Verdächtige Seiten, Werbeanzeigen, Links, Videos, Profile, Apps etc. an die Seitenbetreiber melden, damit diese gelöscht werden.

PHISHING – ACHTUNG VOR DATENKLAW

Beim Phishing versuchen Betrüger über **gefälschte Websites und E-Mails** an Zugangsdaten von Internetnutzer/innen zu kommen. Besonders begehrt sind Accounts für **Online-Banking, Soziale Netzwerke** und **Online-Shops**.

So gehen die Betrüger vor: Du erhältst eine **täuschend echte E-Mail oder Chatnachricht** mit einem Link, über den du dich in deinen Account einloggen sollst (z. B. um dort aus „Sicherheitsgründen“ die Nutzerdaten zu aktualisieren). In Wahrheit wirst du auf eine **gefälschte Website** geleitet, die dem Original zum Täuschen ähnlich sieht. Indem du dich dort einloggst, teilst du den Betrügern deine Zugangsdaten mit. Innerhalb kürzester Zeit können sie so z. B. dein Bankkonto leer räumen, in deinem Namen im Internet einkaufen oder dein Facebook-Profil übernehmen.

TIPP

- Seriöse Unternehmen fragen Kundendaten niemals per E-Mail ab – lösche solche Nachrichten am besten sofort!
- Öffne niemals unbekannte Dateianhänge in Mails (Schadsoftware!).

INTERNET-BETRUG

Infos & Tipps für mehr Sicherheit im Netz



VORSICHT VOR HANDY-ABZOCKE

„500,- Euro-Gutschein zu gewinnen!“, „Besseres WhatsApp möglich“, „Hol dir ein gratis Game!“, „Orte jedes Handy“ – **Werbepanner in Apps oder auf Websites** versprechen so manch tolle Dinge.

Was jedoch viele übersehen: Bei Nutzung dieser „Dienste“ musst du deine Handynummer angeben und **schließt damit oft unbewusst ein ungewolltes Abo ab, für das du zahlen musst**. Den versprochenen „Dienst“ gibt es hingegen nicht. Die Kosten stehen nur **versteckt im Kleingedruckten**. Die böse Überraschung folgt mit der nächsten **Handyrechnung**, auf der teure Mehrwertdienste bzw. WEB- oder WAP-Abos verrechnet werden.

TIPPS

- Sei vorsichtig bei der **Bekanntgabe deiner Handynummer im Internet!** Gewinnspiele oder verlockende Angebote sind oft Abzocke!
- SMS nicht mit „JA“ beantworten, **keine TAN-Codes** übermitteln oder **Bestätigungsbuttons** drücken, wenn kein Abo gewünscht wird.
- Immer die **Handyrechnung** auf ungewöhnliche Beträge kontrollieren.
- Binnen drei Monaten nach Erhalt der Handyrechnung kannst du **Einspruch erheben**. Unter www.rtr.at/schlichtungsstelle bekommst du Hilfe, wenn du Probleme mit deinem Mobilfunkanbieter nicht lösen kannst.
- Vorsichtsmaßnahme: Kostenlose **Sperre** für Mehrwertdienste bzw. WAP-/WEB-Billing bei deinem Mobilfunkanbieter nutzen.

NICHT ALLES IST EIN SCHNÄPPCHEN

Anbieter auf Kleinanzeigen- und Auktionsplattformen, aber auch in unseriösen Online-Shops bieten oftmals **angeblich hochwertige Originalwaren zu einem Bruchteil des üblichen Preises** an. Doch dahinter stecken oft Betrüger, die auf dein Geld aus sind. Trotz überwiesenem Betrag erhältst du **keine Ware** oder die bestellten Artikel entpuppen sich als **billige Markenfälschungen**.

Daher: Finger weg von vermeintlichen Schnäppchen, denn **auch im Internet hat niemand etwas zu verschenken!**

TIPPS

- Sei bei Angeboten vorsichtig, die extrem günstig sind (Preise vergleichen!).
- Bei **Online-Shops aus dem EU-Ausland** sei besonders kritisch, vor allem wenn kaum Angaben zum Verkäufer zu finden sind (Impressum).
- Beim Online-Shopping **vermeide Zahlungen per Vorkasse** mittels Banküberweisung, per Geldtransferdiensten oder per Prepaidkarten. Bei Käufen von Privatpersonen besteh auf eine **persönliche Übergabe**.

WEITERE TIPPS & HILFE!

Internet Ombudsmann: Kostenlose Online-Beratung und Streitschlichtung bei Problemen mit Online-Shopping, Internet-Betrug, Datenschutz & Urheberrecht: www.ombudsmann.at

Watchlist Internet: Aktuelle Meldungen zu Internet-Betrug und Online-Fallen: www.watchlist-internet.at

Impressum/Herausgeber/Kontakt:
Saferinternet.at/ÖIAT, Margaretenstr. 70, 1050 Wien
www.saferinternet.at

Saferinternet.at: Tipps und Infos zur sicheren Internet- und Handynutzung:
www.saferinternet.at/internet-betrug,
www.facebook.com/saferinternetat,
www.instagram.com/saferinternet.at

147 Rat auf Draht: Notruf für Kinder und Jugendliche – rund um die Uhr, anonym, kostenlos. Per Telefon (einfach 147 wählen), Online-Beratung oder Chat: www.rataufdraht.at

Gefördert durch:  
Das Internet sicher nutzen!

Weitere Partner:     

Stand: Dezember 2015