Checkliste: Betrug im Internet bekämpfen

Gut zu wissen:

Die Nutzung von digitalen Medien hat die Lebensumstände massiv verändert und kann viele Erleichterungen und Verbesserungen mit sich bringen. Allerdings sind Nutzer mit einer Technologie konfrontiert, die auch missbraucht wird, neue Gefahrenquellen sind aufgetaucht. Eine regelrechte Betrugsindustrie ist entstanden, die versucht Nutzern auf verschiedenste Arten Geld aus der Tasche zu ziehen. Dabei sind die Methoden immer besser und professioneller geworden. Immer glaubwürdiger versuchen die Betrüger, die Nutzer beispielsweise zur Herausgabe von Daten für einen späteren Angriff auf das Bankkonto, zur Zahlung für Waren bei Fake-Shops oder zu Investitionen in unseriöse Kryptowährungs-Plattformen zu verleiten.

Hier einige Anhaltspunkte, die helfen können, unseriöse Angebote oder Plattformen zu entlarven.

Welche Betrugsformen im Internet gibt es?

Eine Aufzählung kann nur unvollständig sein. Betrüger lassen kaum Möglichkeiten aus ihren Opfern Schaden zuzufügen. Daher hier eine beispielhafte Aufzählung, die noch dramatisch erweitert werden könnte:

- **Phishing Mails oder SMS.** Nachrichten von bekannten Organisationen (z.B. Bank, Post, ÖGK) sind mit der Aufforderung verbunden, Daten einzugeben, etwa Zugangsdaten zum Onlinebanking. Erst in weiterer Folge wird dann der Schaden durch unerwünschte Zahlungen angerichtet.
- **Fake-Gewinne.** Der Gewinn einer Ware oder eines Geldbetrags wird oft mit der Zahlung einer Gebühr für Versendung, Zoll, Notar oder eine andere

Nebentätigkeit verknüpft. Nach der Zahlung ist von dem Gewinn nichts zu sehen.

- **Love-Scamming.** In sozialen Medien oder auf Online-Partnerbörsen werden Nutzer geschickt in eine Falle gelockt. Die interessierte Partnerin oder der verliebte Partner sind aber nur Fake-Profile. Die Opfer werden dann regelrecht mit Geldforderungen gemolken. Etwa durch den angeblichen Arzt aus den USA, der zur Rückzahlung seines Studienkredits Geld braucht, und erst danach nach Österreich kommen kann. Oder es fehlen angeblich die Mittel für das Flugticket. Oder das Opfer soll aus einer anderen finanziellen Notlage helfen.
- **Betrügerische Anrufe.** Anrufer geben sich als Vertreter eines großen Software-Unternehmens aus und verleiten die Opfer, ihnen Zugang zu Computer und Passwörtern zu verschaffen.
- **Betrügerische und irreführende Werbung in Social Media.** Bekannte Personen werden als Werbetestimonials für zweifelhafte Produkte missbraucht, um Verbraucher zu täuschen. Die Empfehlungen durch die Prominenten – etwa einen aus dem Fernsehen äußerst bekannten Arzt – sind jedoch frei erfunden.
- **Versprochene Geschenke.** Per E-Mail wird darüber informiert, dass man hohe Geldsummen oder wertvolle Waren geschenkt bekäme. Für die Abwicklung wird dann aber viel Geld verlangt.
- **Fake-Anzeigen bei Wohnungen oder Autos.** Oft werden Wohnungen günstig angeboten, auch Urlaubsunterkünfte. Wenn dann bereits vorweg eine Geldleistung verlangt wird, stehen die Mieter schließlich vor verschlossenen Türen, wenn sie es mit Betrügern zu tun hatten. Ebenso werden Schnäppchen-Autos angeboten, weil jemand angeblich nach England übersiedelt und der Verkauf so schnell gehen muss. Nach der Vorauszahlung ist von den angeblichen Verkäufern meist nichts mehr zu hören.

- **Phantastische Investitionsmöglichkeiten bei Fake-Krypto-Plattformen.** Der Kryptowährungs-Hype ist in aller Munde. Die Gewinnmöglichkeiten erscheinen grandios, eine Investition kann viel Geld bringen. Leider finden sich in diesem Bereich immer wieder Betrüger. Und dann wartet man vergeblich auf eine Auszahlung, das Investment ist futsch.

Wie kann man betrügerischen Machenschaften auf die Schliche kommen? Wie kann man sich schützen?

Internet-Betrüger sind mittlerweile bestens organisiert. Manche betrügerische Homepage ist höchst professionell gestaltet und erweckt dadurch ein hohes Maß an Vertrauen. Dementsprechend schwierig kann es sein, seriöse von unseriösen Anbietern zu unterscheiden.

- **Ein gesundes Maß an Misstrauen.** Besonders verlockende Angebote sind meist schon verdächtig, oder Gewinnspiele, bei denen man zwar nicht mitgemacht, aber trotzdem gewonnen hat. Wenn ein Angebot fast zu gut ist, um wahr zu sein, dann ist es meist auch nicht wahr. In jedem Fall lohnt es sich, nachzuforschen.
- **Informationen über das betreffende Unternehmen einholen.** Mit einer Suchmaschine lässt sich oft schon viel herausfinden. Bewertungsplattformen können da sehr hilfreich sein. Doch sogar hier gilt es, die Glaubwürdigkeit der Bewertungen kritisch zu hinterfragen.
- **Im Zweifel auch bei Spezialisten nachforschen.** So sind auf watchlist-internet.at zahlreiche Warnungen und Infos zu Internetbetrug zu finden. Unbekannte Shops können auf fakeshop.at/shopcheck überprüft werden.
- **Mit Daten geizen.** Nur die notwendigsten Daten übermitteln, niemals Ausweiskopien oder sensible Daten.
- **Nicht im Voraus bezahlen.** Wer vorher bezahlt, trägt danach das volle Risiko. Mit der richtigen Zahlungsweise, kann Betrug zumindest eingedämmt werden.
- **Auch bei Privatkäufen nicht im Voraus bezahlen.** Betrügerische Machenschaften können auch als Geschäfte unter Privatpersonen getarnt sein. Auch hier ist auf eine sichere Übergabe und sichere Zahlungsmethode zu achten.
- **Bei Nachrichten nicht einfach auf Links klicken.** Betrüger versenden oft E-Mails, die täuschend jenen von seriösen Unternehmen gleichen, auch

manche betrügerische Homepage ist kaum von seriösen zu unterscheiden. Hier sollen die Nutzer oft dazu verleitet werden irgendwelche Links anzuklicken oder anzutippen. Dabei kann aber Unerfreuliches passieren: Die Installation von Schadsoftware, oder ein Social Media-Profil wird gehackt, oder der Abschluss eines kostenpflichtigen Abos wird behauptet. Daher ist es ratsam, solchen Links nicht zu folgen und lieber über einen anderen Weg – etwa über die offizielle Homepage des Unternehmens – die erforderlichen Zugänge zu suchen.

- **Darauf achten, nur die offizielle App herunterzuladen.** Auch mit gefälschten Apps versuchen Betrüger Schadsoftware auf die Geräte zu bekommen, um auf diese Weise etwa Daten auszuspionieren. Bei der Installation von Apps ist daher besondere Vorsicht geboten.
- **Mehrwertdienste am Handy sperren.** Oft verstecken sich in Werbebannern oder Textnachrichten Abo-Fallen. Viele Nutzer merken das erst, wenn bei der Handyrechnung auch Kosten für Mehrwertdienste enthalten sind. Dagegen kann man sich schützen, indem beim Mobilfunkbetreibern Mehrwertdienste gesperrt werden.
- Sofern man **Zweifel** an der Seriosität des Vertragspartners oder des Versenders einer Nachricht hat: **Finger weg.**

Was tun, wenn etwas passiert ist?

Die Professionalität der Internet-Betrüger bedingt leider, dass doch immer wieder Betrugsversuche vom Erfolg gekrönt sind.

- **Versuchen, das Geld zurückzuholen.** Manchmal ist es möglich, Geld wieder zurückzuholen. Es kann daher sinnvoll sein, die Bank und das Kreditkartenunternehmen zu kontaktieren.
- **Informationen einholen.** Möglicherweise haben Experten noch weitere Tipps auf Lager. Die findet man unter ombudsstelle.at oder arbeiterkammer.at.

- **Anzeige bei der Polizei.** Da es sich bei Betrug um eine Straftat handelt, ist eine Anzeige bei der Polizei ratsam.
- **Information beim Bundeskriminalamt.** Das Bundeskriminalamt sieht die Bekämpfung von Internetkriminalität als Schwerpunkt. Daher wurde mit against-cybercrime@bmi.gv.at eine Meldestelle eingerichtet. Eine Meldung dort ersetzt aber nicht die Anzeige bei der Polizeidienststelle.

Weitere Informationen und hilfreiche Links

- arbeiterkammer.at
- ombudsstelle.at
- pishen-impossible.at
- trustedshops.at
- watchlist-internet.at
- fakeshop.at
- Meldestelle BKA: against-cybercrime@bmi.gv.at
- saferinternet.at