Phishing, Trickanrufe und Datenverlust: So kommen Sie sicher durch die digitale Welt

Unsere Gesellschaft ist vernetzter denn je. Die Vorteile, Zahlungen sowie die Kommunikation bequem per Internet oder Smartphone abzuwickeln, sind enorm. Um sicher durch die digitale Welt zu kommen, sind Vorsichtsmaßnahmen wichtig.

Egal ob am Laptop, Computer oder am Smartphone – im Internet suchen wir nach Informationen, kommunizieren und erledigen Einkäufe. Das Bezahlen von Rechnungen ist dabei genauso zum Alltag geworden, wie das Reservieren von Kinotickets. Gerade weil die Nutzung von Internet und Smartphones aus unserem Leben nicht mehr wegzudenken ist, wird der sichere Umgang mit diesen Kommunikationsmitteln immer wichtiger.

Digitale Geräte sicher nutzen

Der Schutz der privaten Daten darf bei der Internet-Nutzung nicht vergessen werden. Wer Regeln wie regelmäßige Software-Updates, eine Firewall und einen Virenschutz beachtet, ist gut geschützt – etwa vor Datenverlust. Empfehlenswert ist, Software-Updates regelmäßig auf dem Gerät zu installieren, denn die neuesten Versionen des Betriebssystems enthalten oft Systemverbesserungen. Um sich vor Malware (so wird Schadsoftware genannt) zu schützen, sollten nur Anwendungen aus den offiziellen App-Shops installiert werden.

Eine Firewall verhindert gefährliche Zugriffe auf Ihren Computer. Moderne Betriebssysteme haben eine Firewall eingebaut, die möglicherweise noch aktiviert werden muss. Ist trotzdem Malware ins System eingedrungen, helfen Anti-Viren-Programme beim Aufspüren. Diese sind in modernen Betriebssystemen bereits integriert. Wichtig ist jedoch, dass sie regelmäßig aktualisiert werden.

Gute Passwörter schützen

Die Verwendung von sicheren Passwörtern gilt als das Um und Auf. Diese bestehen aus einer Kombination aus mindestens acht Buchstaben, Zahlen und Sonderzeichen. Wichtig ist, dass für verschiedene Anwendungen verschiedene Passwörter gewählt werden, die regelmäßig geändert werden.

Neben sicheren Passwörtern wird die Zwei-Faktor-Authentifizierung als zusätzlicher Schutz für Benutzerkonten empfohlen. Dabei muss beim Login zum Passwort etwa ein PIN-Code, der auf das Handy geschickt wird, oder die Zahlenkombination eines Code-Generators eingegeben werden. Auf diese Weise haben Unbefugte keinen Zugriff, selbst wenn sie das Passwort haben.

Vorsicht in den sozialen Netzwerken

Social Media Plattformen wie WhatsApp, Facebook oder Instagram machen es einfach, mit Freunden und Familie bequem in Kontakt zu bleiben. Die geposteten Einblicke in das Privatleben können aber missbraucht werden. Persönliche Daten wie Wohnadresse, Telefonnummer oder Passwörter sollen deshalb nie öffentlich gemacht werden.

Bevor Fotos, Videos oder Texte online gestellt werden, sollte man sich fragen, ob diese später nachteilig für sich selbst oder jemanden anderen verwendet werden könne. Will man Bilder von anderen Personen verbreiten, sollte man diese vorab um Einverständnis fragen – denn es gilt das Recht am eigenen Bild. Wird dieses verletzt, kann die abgebildete Person gerichtlich gegen den Verbreiter des Bildes vorgehen.

Zusätzlich zum umsichtigen Veröffentlichen von persönlichen Einblicken schützen die Privatsphäre-Einstellungen. In den Einstellungs-Optionen kann man den Zugriff auf das Profil beschränken oder

unerwünschte Nutzerinnen und Nutzer blockieren. Es lohnt sich, die Einstellungen regelmäßig zu überprüfen.

So erkennen Sie Phishing-Attacken

Unter dem Begriff „Phishing“ versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben. Waren Phishing-Mails früher oft leicht an den Rechtschreibfehlern zu erkennen, wirken die Nachrichten der „Phisher“ inzwischen häufig wie echte Mails von bekannten Firmen.

Ziel ist es, an die Daten eines Internet-Nutzers zu gelangen. Die möglichen Folgen sind Abbuchungen vom Konto, Identitätsdiebstahl oder die Installation einer Schadsoftware.

Antivirensoftware bietet einen gewissen Schutz vor Phishing. Die wichtigste Regel lautet jedoch, verdächtige Links in Mails nicht anzuklicken. Wird in einem Mail nach dem Passwort oder Zahlungsdaten gefragt, ist Skepsis angebracht. Seriöse Firmen fragen so sensible Daten nicht über E-Mails ab.

Unerwünschte Anrufe, Mails und SMS

In Österreich gibt es ein sehr restriktives Telekommunikationsgesetz. Demnach ist elektronische Kommunikation zu Zwecken der Direktwerbung ohne Zustimmung der Betroffenen untersagt. Denn trotz sorgsamen Umgangs mit persönlichen Daten können diese in falschen Händen geraten und zu unerwünschten Trickanrufen, Werbe-Mails oder Werbe-SMS führen.

Betrügerische Ping-Anrufe – auch Lockanrufe genannt – führen dazu, dass ein „Anruf in Abwesenheit“ einer ausländischen Rufnummer bzw. Satellitenrufnummer aufscheint. Wer zurück ruft, hört in der Regel nur Tonbandansagen, die eine Verbindung möglichst lange aufrechterhalten sollen. Die Geschädigten finden die Kosten auf der nächsten Telefonrechnung.

Die Telekom Regulierungs-GmbH (RTR) ist auf die Bekämpfung von Rufnummernmissbrauch spezialisiert. Wer sich durch Ping-Anrufe oder sonstige störende Anrufe belästigt fühlt, kann die verdächtigen Nummern bei der Behörde melden.

Bei unzulässigen Werbe-E-Mails oder Werbe-SMS ist eine Anzeige beim Fernmeldebüro möglich. Absoluter Schutz kann dadurch jedoch nicht garantiert werden, da Spam – also unerwünschte Mails und Nachrichten – meist von Personen verschickt wird, die sich nicht um rechtliche Vorschriften kümmern.

Mehr Information gibt es unter:

https://www.ombudsstelle.at/ (Zugriff 18.05.2021)

https://www.saferinternet.at/privatsphaere-leitfaeden/ (Zugriff am 16.05.2021)

https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/Beschwerde_Meldung.de.html (Zugriff am 16.05.2021)