21.02.2023

Skriptum

Christina Kössner

Die Sicherheit im Netz ist ganz wichtig.

Gute Ratschläge

Verwendet IMMER ein gutes Virenprogramm! Quelle:
https://www.chip.de/bestenlisten/Bestenliste-Antivirenprogramme-Windows--index/index/id/1451/

Verwendet nicht für alle Zugänge das gleiche Passwort! Sichere Passwörter sollten mindestens 8 Zeichen lang sein, aus Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen und in keinem Wörterbuch zu finden sein oder mit dir in Verbindung stehen. Bei Datenlecks gelangen immer wieder Nutzerkonten und Passwörter in Listen, die sich im Internet verbreiten. Passwörter aufschreiben und manches Mal ändern!

Quelle:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Quelle:
https://www.welivesecurity.com/deutsch/2019/12/10/tipps-speziell-fuer-aeltere-nutzer/

Manche meinen, dass ältere Menschen einem höheren Risiko ausgesetzt sind, auf Betrüger hereinzufallen.

Allein in den USA entsteht Senioren ein Schaden von 3 Milliarden Dollar jährlich. Dies geschieht durch verschiedene Betrügereien wie Diebstahl im Netz und Vertrauensmissbrauch. Diese Zahlen sind jedoch wenig repräsentativ, da die meisten Opfer sich zu sehr schämen, diese Fälle anzuzeigen und somit zuzugeben, dass sie auf einen Betrug hereingefallen sind.

Sei skeptisch!

Vertraue niemals Fremden im Internet. Stattdessen solltest du immer davon ausgehen, dass jede unerwartete Nachricht ein Betrugsversuch sein könnte. Leider muss diese Vorsicht heutzutage auch auf E-Mails bedacht werden, dievon jemandem stammen, den du kennen könntest. E-Mails und deren Absender lassen sich leicht fälschen. Das gleiche gilt für Nachrichten auf dem Handy oder in sozialen Netzwerken wie Facebook & Co. Achte speziell auf eventuelle Ungereimtheiten in Bezug auf den Absender und den Nachrichteninhalt. Im Zweifel lösche die Nachricht. Zur Not kann man sich auch telefonisch bei guten Bekannten rückversichern.

Klicke nichts an!

Phishing Angriffe sind die häufigste Methode, mit denen Kriminelle versuchen, an sensible Daten, wie Kreditkarteninformationen oder Zugangsdaten zu gelangen. Dies geschieht durch perfekt gefälschte Mails, die vorgeben, von der Bank oder vom Online-Dienst zu stammen. Meist bitten diese Mails um „eine Überprüfung deiner Daten“. Gehe auch hier immer von einem Betrugsversuch aus. Klicke weder auf **Links im Mail-Text** und öffne keine **E-Mail-Anhänge.** Deine Bank etwa, wird immer einen echten Brief mit vertraulichen Informationen schicken. Auch hier kannst du dich in den meisten Fällen telefonisch rückversichern.

Niemand hat etwas zu verschenken

Neben Phishing Mails können die Betrüger auch Gewinn-Benachrichtigungen zu angeblichen Preisen schicken. Lotteriegewinne, ohne dass du gespielt hast, oder Lotterien von Firmen wie Coca-Cola sind beliebte Betrugsversuche. Oft wird verlangt, dass du persönliche Daten „bestätigen“ oder vorab eine angebliche Schutz- oder Transaktionsgebühr überweisen sollst, um an deinen vorgeblichen „Gewinn“ zu gelangen. Typischerweise wird im Text zusätzlicher Druck aufgebaut – etwa durch eine ablaufende Zeitspanne. Legitime Lotterien verlangen nie eine Gebühr zur Auszahlung des Gewinns.

Überweise kein Geld an Fremde

Online-Dating-Betrug, bei dem das Opfer dazu gebracht werden soll, Geld oder persönlichste Informationen an die Kriminellen zu senden, war die zweitteuerste Betrugsmasche, auf die Menschen aller Altersklassen im Jahre 2018 hereingefallen sind. Zusammengenommen ist so allein in den USA ein Schaden von 362 Millionen Dollar entstanden. Ein kürzlicher Bericht des FBI zeigt

zudem, dass fast ein Drittel der arglosen Opfer außerdem für Geldwäsche-Kampagnen missbraucht und sie somit ungewollt und unwissentlich zu Verbrechenskomplizen wurden. Betrug rund um Online-Dating-Plattformen ist ganz vorn dabei, wenn es darum geht, vorrangig ältere Menschen auszunutzen. Da gerade Einsamkeit eines der Hauptprobleme im Alter ist, haben Kriminelle oft leichtes Spiel.

Lege auf!

Bei gefälschten Support-Anrufen versuchen Cybergangster, am Telefon davon zu überzeugen, dass dein Computer von einem Virus befallen sei und die Anrufer diesen beseitigen könnten. Dazu müsstest du nur ein kleines Programm herunterladen und ausführen, über das die Anrufenden dann auf deinen PC zugreifen können. Während der Vorwand natürlich gefälscht ist – solche Anrufe sind immer unseriös – stimmt es, dass du mit dem erwähnten Programm außenstehenden Zugriff auf Ihren Computer gewährst. Das nutzen Kriminelle nun aus, um Daten zu stehlen oder erst Schadsoftware, die Bankinformationen ausspionieren soll, händisch zu installieren. Gewähre niemals Fremden, die anrufen, Zugriff auf deinen Computer! Du brauchst auch bei Team Viewer Zugriff von uns keine Angst haben, denn man hat ein Passwort, welches sich bei jedem Öffnen der App verändert. Sage diese Daten aber auch nur zuverlässigen Personen.

Sichere deine Daten!

Die Daten sollten immer abgesichert sein (Cloud oder Externe Festplatte usw.). Falls jemand deinen Computer so schädigt, dass du jederzeit zurücksetzen kannst, ohne deine Daten zu verlieren. Achtung. Externe Festplatte NICHT immer angeschlossen halten. Auch da ist Sicherheit nicht gegeben, wenn jemand eindringt!

Links zur Cybersicherheit zum Nachlesen:

https://www.tagesschau.de/thema/cybersicherheit/

https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/

https://www.techrepublic.com/article/top-cybersecurity-threats/#:~:text=Going%20into%202023%2C%20cybersecurity%20is,attacks%20will%20have%20been%20launched.