8COM
CYBER SECURITY

10 GEBOTE FÜR MEHR CYBER SECURITY

FÜR JUGENDLICHE

1. Bilde dich weiter

Immer schneller schreitet der technologische Fortschritt voran. Was gestern noch als Zukunftsmusik galt, ist heute schon Realität. Doch neue Hard- und Software hat oft Sicherheitslücken – die Kriminelle schamlos ausnutzen. Damit du stets sicher mit den aktuellen Geräten und Programmen umgehen kannst, musst du dich ständig weiterbilden. Achte dabei nicht nur auf die Möglichkeiten und Vorteile neuer Technologien, sondern behalte auch stets ihre Risiken im Auge.

2. Mach deine Geräte zur Festung

Auf deinen Geräten speicherst du unzählige Daten, wahrscheinlich auch Passwörter (das solltest du besser nicht!) oder sensible Fotos und Videos. Genau darauf haben es Cyberkriminelle abgesehen. Denn diese Daten können sie missbrauchen, um sich im Internet als du auszugeben, dich zu erpressen oder öffentlich bloßzustellen. Achte also darauf, dass niemand einfach auf deine Geräte zugreifen kann. Firewalls und Antivirenprogramme helfen dir dabei, Unbefugten den Zugriff auf deine Daten zu erschweren.

Sei außerdem vorsichtig beim Skypen und Chatten: Öffne niemals Dateien, die du nicht erwartet hast oder die dir ein Fremder geschickt hat. Dahinter könnten sich Viren und Trojaner verstecken, mit denen Kriminelle die Kontrolle über deinen Computer übernehmen wollen.

3. Halte deine Software auf dem aktuellen Stand

Firewalls und Antivirenprogramme bringen nichts, wenn sie veraltet sind und aktuelle Bedrohungen nicht erkennen. Dasselbe gilt für jede Art von Software, die nicht auf dem neuesten Stand ist. Installiere Updates für deine Programme also immer, sobald sie veröffentlicht werden. Damit werden gefährliche Sicherheitslücken geschlossen, die Kriminelle ausnutzen könnten, um auf deine Geräte zuzugreifen.

4. Schütze deine Accounts

Wenn es dir wie den meisten Internetnutzern geht, hast du eine Vielzahl von Benutzerkonten bei mehreren verschiedenen Anbietern. Üblicherweise werden diese Accounts mit einem Passwort geschützt. Das Problem: Schwache Passwörter sind mithilfe spezieller Software in Sekundenschnelle geknackt. Deine Passwörter sollten also so stark wie möglich sein. Starke Passwörter sind mindestens 12 Zeichen lang und bestehen aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Verwende auf keinen Fall ganze Wörter, sondern gestalte es so, dass es aussieht, als ob du einfach auf die Tastatur gehämmert hättest.

Verwende außerdem für jedes Benutzerkonto ein eigenes Passwort! So können Kriminelle nur auf jeweils einen Account zugreifen, wenn sie das Passwort knacken. Um deine Konten noch besser vor Missbrauch zu schützen, aktiviere die Zwei-Faktor-Authentifizierung, wann immer dies möglich ist.

8com GmbH & Co. KG | Europastraße 32 | 67433 Neustadt/Weinstraße | www.8com.de | info@8com.de | +49 6321 48446-0

5. Surfe nicht als Admin

Normalerweise meldet sich jeder Benutzer eines Computers mit Benutzername und Passwort an und verfügt damit über ein persönliches Benutzerkonto. Nun sind nicht alle Benutzerkonten gleich; einige dürfen mehr als andere. Sogenannte Admin-Konten (Admin ist kurz für Administrator) haben praktisch uneingeschränkten Zugriff und können Software installieren oder die Systemeinstellungen des Computers ändern.

Viele Computerviren und Trojaner benötigen Admin-Rechte, um einen Rechner vollständig zu infizieren. Da die Schädlinge gewöhnlich über dieselben Berechtigungen verfügen wie der Benutzer, der sie sich unfreiwillig eingefangen hat, solltest du niemals als Admin im Internet surfen oder E-Mails versenden und empfangen. Erstelle dafür am besten ein eigenes Benutzerkonto ohne Admin-Rechte. Das machst du in wenigen Schritten über die Benutzerkontenverwaltung deines Computers.

6. Sei vorsichtig beim Surfen

Im Internet tummeln sich viele Kriminelle, die ständig versuchen, dich hinters Licht zu führen. Sie wollen, dass du Zugangsdaten auf gefälschten Webseiten eingibst oder gefährliche Schadprogramme herunterlädst, die als vermeintlich harmlose Dateien getarnt sind. Sei also stets aufmerksam, wenn du im Internet unterwegs bist.

Achte darauf, dass die Verbindung zwischen deinem Gerät und einer Webseite verschlüsselt ist. Das erkennst du meistens am Kürzel „https://“ vor der Adresse der Webseite oder an einem Vorhängeschloss-Symbol in der Adressleiste des Browsers. Apropos Browser: Die solltest du natürlich auch regelmäßig updaten. Es empfiehlt sich außerdem, immer zwei Browser installiert zu haben. Wenn Sicherheitslücken in einem gemeldet werden, benutzt man den anderen, bis die Lücken durch Aktualisierungen geschlossen wurden.

7. Schalte aus, was du nicht brauchst

Kabellose Verbindungen sind zwar ungemein praktisch. Sie machen es Kriminellen aber auch einfacher, auf deine Geräte zuzugreifen und deine Aktivitäten nachzuverfolgen. WLAN, GPS, Bluetooth und NFC solltest du also immer ausschalten, wenn du sie gerade nicht brauchst. Damit schützt du dein Gerät nicht nur vor unbefugtem Zugriff, sondern schonst zusätzlich den Akku. Denn was ausgeschaltet ist, verbraucht auch keinen Strom.

8. Schütze deine Privatsphäre

Du hast ein Facebook-Profil und postest gerne Bilder, Kommentare und andere persönliche Informationen? Dann solltest du gut aufpassen, wer sie sehen kann. Schau mal in die Privatsphäre-Einstellungen. Da kannst du festlegen, wer welche Inhalte von dir sehen darf. Das gilt auch für alle anderen sozialen Netzwerke und Chat-Programme, die du benutzt. Über das Internet versuchen Cyberkriminelle oft, an vertrauliche Daten zu kommen. Sei misstrauisch und gib niemals persönliche Informationen oder intime Fotos weiter.

8com GmbH & Co. KG | Europastraße 32 | 67433 Neustadt/Weinstraße | www.8com.de | info@8com.de | +49 6321 48446-0

9. Glaub nicht alles, was du liest

Nicht alles, was im Netz steht, ist wahr. Oft stößt man einfach nur auf Blödsinn. Aber auch Lügen werden dort bewusst verbreitet. Solche Falschmeldungen nennt man Fake News. Sei deshalb immer misstrauisch gegenüber dem, was du im Internet findest. Kommt dir irgendetwas seltsam vor, schau lieber noch einmal in einer anderen Quelle nach und mach deinen eigenen Faktencheck.

10. Cybermobbing: Schau nicht weg!

In sozialen Netzwerken kann man Menschen schnell mit Worten verletzen. Die Folgen sind nicht abschätzbar. Achte daher immer auf einen freundlichen und höflichen Umgang. Bemerkst du, dass jemand in sozialen Netzwerken gemobbt wird, dann greif ein. Sag es deinen Eltern, Lehrern oder der Polizei und sammle Beweise. Cybermobbing wird sogar strafrechtlich verfolgt. Dafür ist Beweissicherung sehr wichtig, z. B. durch ausgedruckte Screenshots und E-Mails.

8com GmbH & Co. KG | Europastraße 32 | 67433 Neustadt/Weinstraße | www.8com.de | info@8com.de | +49 6321 48446-0