Proseminar zum Safer Internet Day am 9. Februar: Tipps für ein (nicht nur) sicheres Studium

Im Augenblick sitzen nicht nur Schüler und Arbeitnehmer in Heimarbeit, sondern auch Studenten. Nach Tipps zu Homeoffice und Homeschooling, die am Ende dieses Artikels noch einmal verlinkt sind, widmet sich Sophos zum Safer Internet Day dem wissenschaftlichen Nachwuchs: wie lässt sich das Online-Studium sicherer gestalten.

Ein Studium ohne Computer ist selbst in den anwendungsorientiertesten Fächern kaum möglich. Er dient der Datenerfassung, Recherche, dem Schreiben von Hausarbeiten und Tests und schlichtweg auch der Kommunikation. Internet und Computertechnologie sind auch jenseits technischer Studiengänge essentieller Bestandteil der Hochschulausbildung. Alarmierend ist jedoch der sorglose Umgang mit drohenden Cybergefahren.

Der Safer Internet Day am 9. Februar ist ein willkommener Anlass, sich in Sachen Cybersicherheit noch einmal mit den wichtigsten Maßnahmen auseinanderzusetzen:

1. HTTPS Webseiten sind am sichersten
Die Internetnutzung ist generell aufgrund der derzeitigen Situation stark gestiegen, Homeoffice und Homeschooling bzw. Homestudying und auch der Kontaktpflege sei Dank.
Bei der Recherche für Themen und Aufgaben bietet es zwar eine schier unerschöpfliche Vielfalt an Material, aber ist jede dieser Seiten auch eine sichere Quelle? Quick-Check: verwendet die Webseite HTTPS (also ein sicheres Protokoll, erkennbar am Schloss in der Adresszeile)? Viele Studenten kennen den Unterschied zwischen sicheren und normalen HTTP-Webseiten nicht. Aber, selbst wenn auf einer unsicheren Webseite nach Passwörtern oder persönlichen Informationen gefragt wird, warnen die meisten Browser mittlerweile vor der Eingabe dieser, denn Daten in unsicherem Web-Traffic können schnell ausgeschnüffelt werden, während sie durchs Internet reisen. Der Verlauf der Webseiten-Besuche gibt auch Hinweise auf das Nutzerverhalten und das geht niemanden etwas an.

2. Vorsicht vor Betrügern
Studenten erhalten oft viele E-Mails zu Lektüren, Seminaren, Aktivitäten von Studentenvereinigungen und sonstigen Themen rund um die Universität. Angesichts dieser Flut ist es wichtig, wachsam zu bleiben – besonders wenn man um irgendeine „Handlung“ gebeten wird. Links, Downloads, Installation von Apps oder Ändern von Einstellungen – hier sollten Alarmglocken klingeln. Um sich vor Betrug und Phishing zu schützen, sollte man die Identität des Absenders absolut sicher kennen. Wenn die Weitergabe persönlicher Daten gefordert wird, hilft der Grundsatz: „If in doubt, don‘t give it out“.

3. Platz verlassen – dann PC ausschalten
Bibliotheken sind (zumindest außerhalb der Corona-Zeit) der natürliche Wirkungsraum vieler Studenten. Wer seinen Arbeitsplatz, ob Desktop-Computer oder eigenen Laptop, zum Beispiel in Richtung Kopierer verlässt, sollte sich ausloggen oder den Screen sperren. Empfehlenswerter als die Autolock-Funktion der Geräte ist übrigens der manuelle Hotkey, da er sofort greift. Für Windows gilt das mit Windows+L, Mac reagiert auf Control+Command+Q.

4. Ein guter Passwort-Manager ist Pflicht
Ein guter Passwort-Manager organisiert den Zugang zu den unzählbaren Accounts, von Social Media über E-Mail-Konten zu diversen Portalen. Will man sich das alles selbst merken, werden

die Passwörter oft zu simpel und ein Passwort muss für mehrere Konten herhalten. Ein unsicheres Vorgehen, wie man eigentlich weiß.
Der Passwort-Manager wählt und organisiert automatisch starke und unterschiedliche Passwörter für jeden einzelnen Account. Weiterer Vorteil gegenüber Phishing-Attacken: der Passwort-Manager „erinnert“ sich an die korrekte Webseite und bemerkt Fake-Phishingseiten.

5. Sichere Online-Käufe
Ob Lehrmaterial, Kleidung, Hobbyartikel oder technisches Equipment – vieles wurde bereits vor Corona online bestellt und gilt jetzt natürlich noch mehr. Auch hier bitte merken: Zweifel bei einem bestimmten Anbieter? Dann lieber keine Bankdaten eingeben. Wichtige Grundregeln für das ganzjährige Online-Shopping hat Sophos unter Black Friday: Stay Safe before, during and after Peak Retail Season zusammengefasst.

Schlussanmerkung: Mach dir keinen (Cyber)Stress
Ein Studium ist aufregend genug, auch ohne Cyberbedrohungen. Mit diesen einfach umzusetzenden Tipps kann man seine wissenschaftliche Arbeit, ob virtuell oder (irgendwann) wieder vor Ort, sicherer gestalten und sich nicht nur auf Theorie und Forschung konzentrieren, sondern auch seine privaten Daten schützen.

Hier gibt es weitere Tipps für sicheres Homeschooling.

Hierunter finden sich Tipps für ein sicheres Homeoffice.

So kann man sein Wi-Fi noch einmal auf fünf Sicherheitseinstellungen überprüfen.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de