SOPHOS

Schulbeginn: die Social-Media-Drähte glühen. Sophos gibt Tipps für den sicheren Umgang mit Social-Media-Profilen – nicht nur für Schüler.

Ferienende in Deutschland, nach und nach fängt nun in allen Bundesländern die Schule wieder an. Und mit ihr Lust und Frust rund um den Schulalltag, das Kichern und Tratschen, Schwärmen und Schwelgen. All das wird von Schülern aller Altersklassen gern auf unterschiedlichen Social-Media-Kanälen geteilt. Die Datensicherheitsexperten von Sophos geben Schülern – und natürlich nicht nur diesen – einige Tipps zum sicheren Umgang mit ihren Social-Media-Profilen.

1. Was Du nicht im persönlichen Gespräch sagen würdest, das teile auch nicht online.

Überlege genau was du postest und teile im Zweifel lieber weniger. Denn alles, was nicht per Einstellung nur für die Augen von Freunden bestimmt ist, kann von jedem gesehen und missbräuchlich verwendet werden. Dazu kommt, dass die Inhalte, die online oder per App geteilt werden, eine lange Lebensdauer haben – das Netz vergisst nichts.

Deshalb: lasse größte Vorsicht walten beim Teilen von persönlichen Dingen. Und selbst wenn deine App dir mitteilt, dein Post sei erloschen, sei dir bewusst, dass es für Hacker immer Mittel und Wege gibt, an deine privaten Posts zu kommen.

2. Poste nur im privaten Modus und halte dein Profil nur Freunden vor.

Überprüfe die Privatsphäre-Einstellungen deiner Social-Media-Konten. Es ist ratsam, Facebook oder Instagram Profile wirklich nur für Freunde und/oder auf Einladung freizugeben, damit du jederzeit einen Überblick darüber hast, wer deine Posts sehen kann. Die Social Media Plattformen bieten viele Optionen für deine Datenschutzeinstellungen – bleib hier auf dem Laufenden und prüfe diese regelmäßig, um dein Profil anzupassen.

Halte dich an folgende Regel: Alles, was in den Social-Media-Kanälen geschrieben wird, sollte nur für ein selbst ausgewähltes Publikum sein. Außerdem ist es aus Sicherheitsgründen besser mit Informationen wie Standort, E-Mail-Adressen oder persönlichen Daten extrem zu geizen.

3. Nimm den Begriff „persönliches Passwort“ wörtlich – und zwar für jedes Profil.

Dein Passwort sollte ausgeklügelt und raffiniert sein und es sollte ganz allein dein Geheimnis bleiben. Und: du solltest für jedes Profil und jeden Online-Account ein solches Passwort entwickeln. Es ist zwar bequem und praktisch, ein wirklich gut ausgedachtes, sicher scheinendes Passwort für alle Profile zu benutzen, doch tatsächlich passiert es öfter als gedacht, dass Hacker es doch schaffen, in ein Profil einzudringen – und damit Zugang zu allen anderen Profilen zu erhalten, die du irgendwo angelegt hast.

Also: Online-Accounts, Social-Media-Profile etc. benötigen jeweils ein eigenes, kluges Passwort. Außerdem vermeide es unbedingt, dein Passwort mit Freunden zu teilen – etwa um dem vertrauten Menschen Zugang zum eigenen Facebook-Profil zu gewähren. Wird nämlich beispielsweise das Handy der besten Freundin mit den Zugangsdaten zu deinem

Facebook-Profil geklaut, können Fremde deinen Account verwenden. Und wenn du Pech hast, dich beispielsweise mit peinlichen Posts bloßstellen.

4. Lade nicht alles herunter und klicke nur an, was du kennst.

Genauso, wie du deinem Körper sicher nicht zumuten möchtest, jeden ungesunden Mist zu essen, solltest auch bei deinem Smartphone sorgsam mit dem umgehen, was du ihm zuführst. Apps, die Schadware enthalten, können im Zweifel dein Handy oder deinen Computer auf Nimmerwiedersehen lahmlegen, es können damit deine eigenen privaten Daten oder die deiner Familie und Freunde ausgelesen werden und vieles mehr. Daher gilt: niemals auf lustig aussehende E-Mails mit Downloadfunktion klicken, keine unbekannte App sorglos herunterladen und keine kostenlose Software installieren von einer Website, die du nicht kennst.

Am sichersten bewegst du dich in offiziellen Apps-Stores und bei seriösen Anbietern von freier Software.

5. Ausloggen. Verschließen.

Wenn du den Besuch deines Social-Media-Profils beendet hast, logge dich immer aus. Dies gilt ganz besonders, wenn du einen anderen als deinen eigenen Computer oder dein eigenes Smartphone benutzt hast – also etwa den Computer in einer Bibliothek, in der Schule, der Uni oder anderswo. Der nächste Nutzer des Computers könnte ansonsten freien Zugang zu deinen E-Mails, deinem Facebook-Profil, deinem App-Store etc. haben. Kein schöner Gedanke.

Du solltest darüber hinaus dafür sorgen, dass du auch aus deinem Smartphone „ausgeloggt“ bist, wenn du es nicht benutzt. Sichere es mit einem Passwort, sodass ein Fremder oder auch ein Freund keine Möglichkeit bekommt mit deinem Gerät zu chatten, zu telefonieren, in deine Social-Media-Profile zu posten, Onlinekäufe zu tätigen, etc.

Mit einem Passwort verhinderst du Datenverlust und -Missbrauch, Schabernack von Freunden und machst dein Smartphone außerdem für Diebe unbrauchbar. Für noch mer Schutz gegen die fiesen Tricks der Cyberkriminellen stehen eine Reihe guter, kostenloser Schutzprogramme zur Verfügung, wie etwa Sophos Home. Es bietet Sicherheit für bis zu 10 private Rechner und wird zentral über den Browser verwaltet.

Mit diesen einfachen Vorsichtsmaßnahmen kannst du dich nach Ferienende beruhigt wieder mit deinen Freunden online treffen – ohne mit bösen Überraschungen rechnen zu müssen.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de