12 TIPPS, UM IHR HANDY VOR ANGRIFFEN ZU SCHÜTZEN

Quelle: http://www.sicher-stark-team.de/

Tipp 1: **Updates**
Genauso wie am Computer sind aktuelle Updates sehr wichtig. Viele Handys sind heute noch immer mit der ersten Software, die beim Kauf erworben wurde, ausgestattet und wenige Kinder und Erwachsene halten ihr Handy auf dem neuesten Stand. So nutzen Hacker die Sicherheitslücken, um Zugriff zu erlangen.

Tipp 2: **Codierung nutzen**
Bei den neueren Handys können Sie Ihre Daten verschlüsselt verschicken. Sie sollten immer persönliche Daten, Anmeldedaten, E-Mails und Websites verschlüsselt übertragen. Mails können beispielsweise mit Hilfe von Apps wie dem „Android Privacy Guard“ vor dem Senden unleserlich gemacht werden. Während die Daten übertragen werden, kann dann niemand mithören.

Tipp 3: **Achten Sie auf das richtige Smartphone**
Jeder Hersteller hat seine Vor- und Nacheile. Informieren Sie sich vor dem Kauf. Die vier gängigsten Smartphones sind Googles Android, Apples iPhone, Blackberry und Microsofts Windows Phone 8. Laut Testergebnissen sind die iPhones und das Windows Phone 8 zur Zeit die sichersten Systeme, was sich aber jederzeit wieder ändern kann.

Tipp 4: **Zugangscode aktivieren**
Nach Kauf sollten Sie auf jeden Fall die Sperrmöglichkeiten, die das Handy bietet, nutzen. In der Regel Pincodesperre und Kartensperre auf „aktiv“ setzen, um es vor Fremden zu schützen. Auch die Displaysperre/Tastensperre sollten Sie aktivieren, sodass das Handy in der Tasche sich nicht selbst aktiviert und sich mit dem Internet verbindet oder jemanden unbeabsichtigt anruft.

Tipp 5: **Vorträge besuchen**
Informieren Sie sich frühzeitig auf Vorträgen/Workshops über die neuen Gefahren und den Schutz für Ihr Handy/ Ihren PC und mobile Geräte. Auch Ihre Kinder sollten Sie in diese Sicherheitsthemen einbeziehen. Das Sicher-Stark-Team bietet seit Jahren deutschlandweite Vorträge unter http://www.sicher-stark-team.de/sicher-stark-vortraege.cfm an.

Tipp 6: **Bluetooth abschalten**
Gerade Bluetooth-Verbindungen lieben Hacker als Einfallstor. Schalten Sie generell Funkdienste ab, wenn sie nicht gebraucht werden. WLAN, GPS und Bluetooth brauchen Sie bestenfalls bei Google Maps und Datenabgleich mit anderen Handys. Deshalb, wenn Sie nicht unbedingt diese Funktion nutzen, abschalten. So können Fremde keinen Zugriff erlangen.
Sie kosten außerdem unnötig Strom.

Tipp 7: **Hotspots beachten**
Gerade öffentliche Internet-Hotspots bieten nur wenig Sicherheit.
Leider können Sie nur selten prüfen, ob ein Hotspot wirklich der ist, der er vorgibt zu sein. Hacker können gefälschte Zugangspunkte installieren: Wenn Sie diese dann mit Ihrem Handy nutzen, können die Gauner mithören oder persönliche Zugangsdaten abgreifen.

Tipp 8: **Fremde Rufnummern**

Bevor Sie eine Rufnummer zurückrufen, sollten Sie prüfen, ob es sich um eine kostenpflichtige Mehrwertrufnummer handelt. In der heutigen Zeit ist es gar kein Problem, mehrere Rufumleitungen zu legen, was Mehrkosten verursachen kann.

Sofern möglich, sollten Sie einen Einzelverbindungsnachweis für Ihre Telefonrechnung beantragen. Prüfen Sie die Abrechnung sehr genau. Dort finden Sie sofort teure Mehrwertrufnummern.
Wenn Sie Kinder haben, sollten Sie kostenpflichtige Mehrwertdienste und mobilen Zahlungsverkehr für das Kinderhandy sperren lassen. Dann gibt es keine bösen Überraschungen mehr am Monatsende.

Tipp 9: **Niemals SMS und MSM von Fremden anklicken**
Wenn Sie ganz sicher gehen wollen, sollten Sie niemals auf Links in SMS, E-Mails oder anderen Nachrichten klicken. Leider nutzen Cracker dies als Einfallstor, um das Handy mit Malware anzugreifen oder zu infizieren. Danach kann der Hacker nach Lust und Laune alle Funktionen in Ihrem Handy bedienen und abrufen. Öffnen Sie MMS auch nur, wenn Sie sicher sind, dass die Bildnachricht von der Person kommt, die sie geschickt haben soll. Zur Not rufen Sie kurz vorher an.

Tipp 10: **Apps**
Installieren Sie nur vertrauenswürdige Apps. Jede App will verschiedene Funktionen Ihres Smartphones nutzen, beispielsweise die Internetverbindung oder die Daten Ihres Adressbuches. Während der Installation muss jede App zunächst fragen, ob der Nutzer damit einverstanden ist. Vergeben Sie diese Rechte nur dann, wenn Sie sicher sind, dass die App aus vertrauenswürdigen Quellen stammt, denn hinter einigen Apps verstecken sich Viren. Im Zweifel nehmen Sie von der Installation Abstand und suchen nach einer anderen App. Installieren Sie zunächst Apps, die Viren auf Ihrem Smartphone ausfindig machen können.

Tipp 11: **Diebstahl**
Sollte Ihr Handy einmal gestohlen werden, so aktivieren Sie von einem anderen Handy den Löschcode. Die neueren Smartphones haben diese Funktion bereits installiert. Bei älteren Geräten können Sie dies durch eine App nachrüsten. F-Secure bietet für Smartphones und Tablets bereits solche Apps an. Auch eine Sperre der Kinder-Smartphones kann so durchgeführt werden. So können Sie immer im Notfall aus der Ferne sämtliche Daten löschen, sodass sie für den Dieb unbrauchbar sind.

Tipp 12: **Backups**
Und denken Sie auch daran, immer regelmäßig Backups zu machen. Sollte das Handy verloren gehen, spielen Sie die Sicherungskopie einfach auf Ihr Handy zurück.

Dipl.-Päd. Gudrun Müller

Fachdienst 40 - Schule und Sport -
Datenschutzbeauftragte für Schulen
Medienrecht für Schulen
Kreisverwaltung Recklinghausen
Medienzentrum Marl
Lehmbecker Pfad 31
45770 Marl