POLIZEI
Nordrhein-Westfalen
Kreis Lippe

bürgerorientiert · professionell · rechtsstaatlich

Smartphone & Co.

Präventionstipps zum Thema Sicherheit für Smartphone, Tablet und anderen Computern

Dein Verhalten…

… mein Smartphone ist mein Smartphone: Das Smartphone ist ein Computer voll mit Apps, persönlichen Daten und Inhalten. Gebt das Smartphone nicht unbeaufsichtigt aus der Hand. Schad- bzw. Spionagesoftware könnte installiert werden.

… Privatsphäre-Einstellungen von Apps überprüfen: **Wer** darf mich **wo** sehen ist hier die Frage. Freunde, Freunde von Freuden oder Jeder. Das Letztere ist wohl die schlechteste Wahl und wird nicht empfohlen. Jeder kann dich anschreiben, dir Nachrichten und Bilder senden. Sogenannte „Groomer“ könnten versuchen mit dir in Kontakt zu treten. Ihr Ziel ist es sexuelle Kontakte zu dir aufzubauen. Dabei geben sie sich oft als Gleichaltrige aus, sind es aber nicht. Mit Chatfunktion ausgestattete Apps und Spiele sind potentielle Spielfelder für Groomer. Schreiben solltest du nur mit Personen, denen du schon einmal die Hand geschüttelt hast.

... unbekannte Telefonnummern: Solltest du erst einmal kritisch betrachten. Sie tauchen nicht in deinen Kontakten auf und sind erst einmal Fremde die dich kontaktieren. Gerade auch bei WhatsApp solltest du darauf achten. Informiere deine Erziehungsberechtigten und lösch die Nachricht.

… sei sparsam mit deinen persönlichen Daten und Informationen über dein persönliches Umfeld:

Viele Betrüger sammeln Daten über ihre potentiellen Opfer. Sie gaukeln Freundschaft vor und fragen dich nach vielen Dingen aus. Wo arbeitet dein Vater, wann fahrt ihr in den Urlaub, wo wohnt deine Oma. In der Wirtschaft nennt man das „Social Engineering“. Einfach gesagt Beeinflussung durch einfachste Kommunikation. Gebt nicht zu viele Informationen preis und seid skeptisch.

… den Klick auf Links vermeiden: Gerade in E-Mails und SMS sind Links sehr gefährlich. Beim Klick auf diese wird immer eine Aktion ausgelöst, die

du nicht kontrollieren kannst. Bei E-Mails solltest du den Absender schon kennen. Bei einer SMS oder einer Messenger-nachricht ist dies zu 90% ein Betrugsversuch. Der Mouseover-Effekt[1] funktioniert beim Smartphone nicht gut.

Deine Technik deine Sicherheit:

… ein Antivirenprogramm ist nicht nur für den PC oder Laptop wichtig. Es schützt auch dein Smartphone vor kriminellen Machenschaften.

…Updates schließen Sicherheitslücken von Apps und Betriebssystem. Stellt wenn möglich eure Computer und Smartphones auf „Updates automatisch installieren“ ein.

…Passwörter: mindestens 10 Stellen, Groß- und Kleinbuchstaben, Sonder-zeichen und Zahlen. Wann immer möglich Zwei- oder Mehrfaktorauthentifizierung benutzen.

… unverschlüsseltes WLAN nicht nutzen: Niemals ohne eine Ver-schlüsselung im Internet surfen. Un-verschlüsselte Kommunikation kann mitgelesen werden. (Zugangsdaten, Passwörter, etc.).

Ein verschlüsseltes WLAN erkennt ihr an folgenden Symbolen.

… VPN benutzen: Ein VPN[2] stellte eine verschlüsselte Verbindung (Tunnel) zwischen deinem Endgerät und einer Website her, auch wenn kein verschlüsseltes WLAN vorhanden ist. Außerdem wird dein Standort nicht freigegeben.

… die Verschlüsselung von Smart-phone, Laptop, USB-Stick und Fest-platten hilft dir bei Diebstahl. Deine Daten können nicht eingelesen werden

… aktuelle Sicherungen helfen dir deine entwendete Hardware, Daten und Dokumente wieder herzustellen.

… IMEI und Kopie der Rechnung von deinem Smartphone solltest du griffbereit haben, falls du bei der Polizei eine Anzeige wegen Diebstahls aufgeben möchtest.

Anzeige bei jeder Wache der Polizei oder unter: https://internetwache.polizei.nrw/

---

[1] Sobald der Nutzer zum Beispiel mit dem Maus-Zeiger oder einem digitalen Stift über ein mit dem Mouse Over Effekt versehenes Element fährt (Trigger Bereich), verändert sich dieses. Der Mouseover-Effekt bei einem Link zeigt die wirkliche Adresse an.

[2] VPN = „Virtual Privat Network“ stellt in diesem Fall eine sichere Verbindung zwischen einer Website und deinem Endgerät her.