Smartphones

Gängige Betrugsmaschen erkennen

In unserer Gesellschaft gibt es mehr Smartphones als PCs. Kein Wunder, denn die kleinen Geräte sind selbst Hochleistungscomputer, die uns rund um die Uhr mit Freunden, Familie und, wenn wir wollen, mit der ganzen Welt verbinden. Telefonieren war gestern – heute wird mit dem Handy gesimst, getweetet und gechattet, was das Zeug hält. Wieviel Potenzial in den kleinen Geräten steckt, haben jedoch auch Betrüger längst entdeckt…

Die Betrugsmaschen

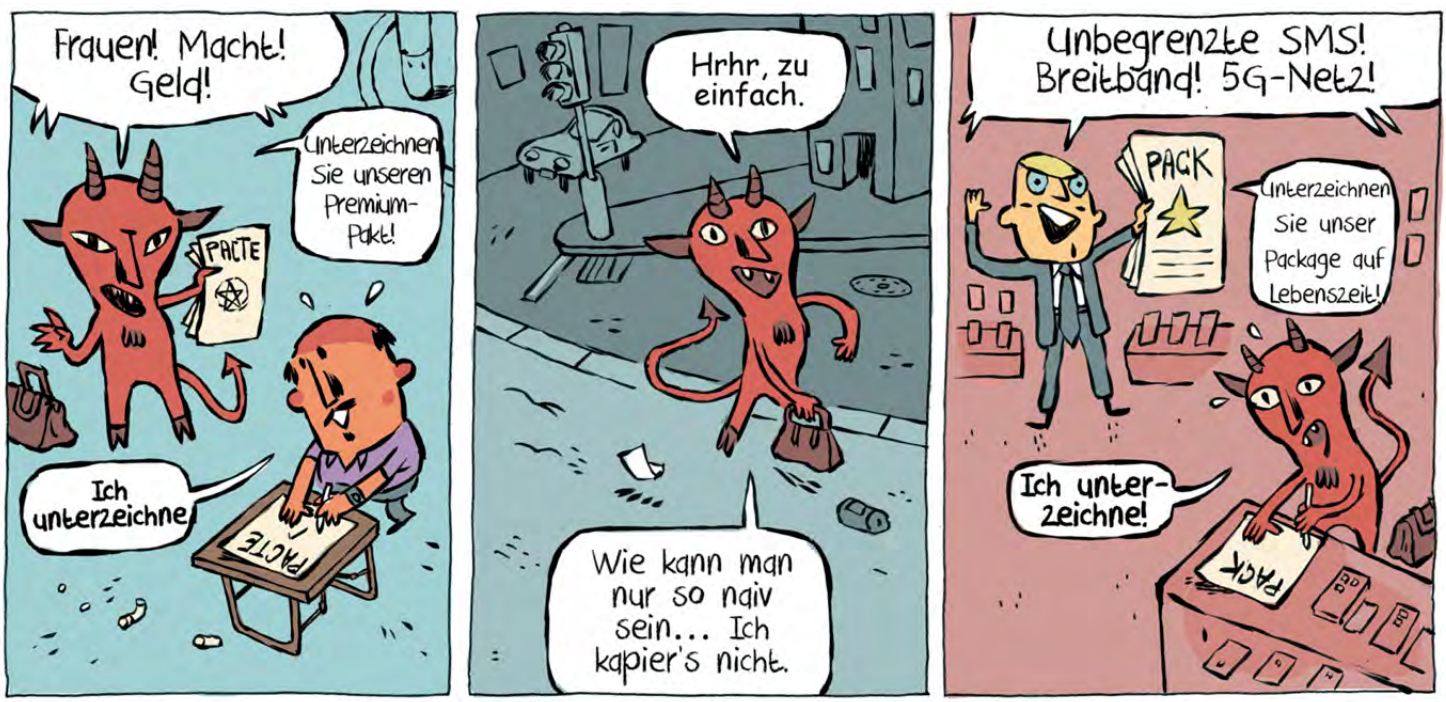
Abofallen & Premium SMS

Teure Abonnements kommen schnell und leider oft unbemerkt zustande. Etwa, indem der Benutzer vom Angebot einer Webseite profitiert, über das Handy zu bezahlen. Dazu gibt er seine Telefonnummer online ein und erhält schnell eine Bestätigungs-SMS und den Zugriff auf den gekauften Inhalt. Eine andere Möglichkeit zum Beziehen von Inhalten (z.B. Handygames, Teilnahme an Gewinnspielen) ist das Senden einer Premium-SMS. Diese kann bis zu 5 Euro zzgl. dem regulären Versandpreis kosten.

Was der Benutzer meist nicht weiß: Er hat ein Abo abgeschlossen, das richtig teuer zu Buche schlagen kann. In regelmäßigen Abständen (z.B. einmal pro Woche, oder alle 3 Tage) werden anfallende Kosten über die Handyrechnung eingezogen.

Auch wenn er noch so langweilig ist, sollte man IMMER den Vertrag eines Handydienstes lesen, bevor man etwas bestellt. So weiß man wenigstens genau, was man wie teuer bezahlt und inwiefern man sich verpflichtet. Wer unerwünschte SMS- oder MMS-Abos stoppen möchte, sollte eine SMS mit dem Text „STOP“ an die Absendernummer schicken (bzw. an die Nummer, die in den Kündigungsmodalitäten angegeben wird). Kommt keine Bestätigungsnachricht, kann man den Dienstleister schriftlich kontaktieren.

Beim Provider kann man eine Drittanbietersperre beantragen, die kostenpflichtige Premium-SMS von vornherein sperrt.



Überteuerte Rufnummern

Im Internet trifft man immer wieder auf Anbieter, die z.B. Handy-Inhalte, Wetterinfos oder Verkehrsmeldungen gegen Bezahlung zum Download anbieten. Bestellen kann man sie oft über eine fünfstellige Premiumnummer.

Hierbei handelt es sich um überteuerte Rufnummern, die mehrere Euro pro Minute kosten. Hinzu kommt, dass die Anbieter mit allen Mitteln versuchen, den Anrufer so lange wie möglich in der Leitung zu halten, um die Kosten in die Höhe zu schrauben.

Beim Provider kann man eine Drittanbietersperre beantragen, die kostenpflichtige Mehrwertdienstnummern von vornherein sperrt. Ansonsten gilt: Herausfinden, was die Kommunikation kostet, BEVOR man anruft. Sind die Kosten hoch, handelt es sich um eine Abzocke, von der man besser die Finger lassen sollte.

Handy-Mafia?

Ihr Handy ist weg – verloren oder geklaut. Bei der nächsten Telefonrechnung kommt der Schock: eine fünfstellige Summe geht auf Ihre Kosten!

Spezialisierte Handydiebe haben es längst nicht mehr auf das Gerät an sich abgesehen. Stattdessen werden mit einem gestohlenen Handy im Sekundentakt kostenpflichtige Hotlines angerufen. Hotlines, die von der kriminellen Bande eigens zu diesem Zweck eingerichtet wurden, und deren Erträge sofort auf die Konten der Diebe fließen.

Wenn Sie merken, dass Ihr Handy weg ist, lassen Sie *sofort vom Provider die SIM-Karte sperren. Je länger dies dauert, umso höher wird die Handyrechnung. Dokumentieren Sie, wann Sie den Verlust Ihres Handys bemerkt und den Provider darüber informiert haben. Im schlimmsten Fall müssen Sie für die Anrufe der Kriminellen selber aufkommen.*

Grundsätzlich sollten Sie die Bildschirmsperre auf Ihrem Handy aktivieren. Nach mehrfacher Eingabe eines falschen Codes wird das Gerät gesperrt. Im Ernstfall gewinnen Sie so zumindest etwas Zeit und können den Schaden entweder eindämmen oder sogar ganz verhindern.

Beim Provider können Sie beantragen, dass Premium-Nummern von vornherein gesperrt werden. So sind Sie gegen diese Art von Betrug gewappnet.

In-App-Käufe

Sie sind ganz begeistert von Ihrer neusten Smartphone-App. Doch nach drei Stunden Dauerspielen kommt der erste Frust: So richtig weiter kommen Sie mit Ihrer Spielfigur nicht mehr. Es sei denn, Sie reagieren auf eines der Popups, das immer wieder auftaucht, und das Ihnen für ein paar Euro viele Spiele-Extras und neue Level verspricht…

Eine richtige Betrugsmasche sind In-App-Käufe nicht. Eine Kostenfalle sind sie aber allemal! Viele vermeintlich kostenlose Apps finanzieren sich durch In-App-Verkäufe. Dies bedeutet, dass das Installieren und primäre Benutzen der Applikation zwar gratis ist, richtiger Nutzen aber nur dann aufkommt, wenn man zusätzliche Inhalte (z.B. „Leben“, Spielgeld, Items,…) für echtes Geld dazu kauft. Meistens bleibt es auch nicht bei einem einzigen Kauf, so dass sich die Ausgaben summieren.

Solange Sie den Überblick über Ihre Einkäufe bewahren, und sich bewusst sind, dass diese echtes Geld kosten, ist alles in Ordnung. Problematischer sind In-App-Käufe, wenn sie von Kindern getätigt werden. Diese sind sich meist nicht bewusst, was genau sie da machen und geben im Eifer des Gefechts schnell mehr aus, als den Eltern lieb ist. Hier hilft nur: Kinder über In-App-Käufe aufklären, die Einkauffunktion im Appstore mit Passwort schützen oder die Funktion der In-App-Käufe in den Einstellungen des Smartphones komplett sperren.

Apps, die unbemerkt teure Anrufe tätigen

Sie haben eine Gratis-App heruntergeladen. Am Ende des Monats stellen Sie beim Blick auf die Handyrechnung fest, dass Sie Premium-SMS verschickt haben, beziehungsweise mehrmals eine teure Mehrwertdienstnummer angerufen haben. Wissentlich haben Sie das jedoch nicht getan…Kann es vielleicht an der neuen App liegen?

Ja! Immer öfter werden Apps entlarvt, die zwar beim Download gratis sind, jedoch im Hintergrund teure SMS verschicken und Anrufe tätigen. Davon bekommt das Opfer nichts mit und merkt es (wenn überhaupt) erst beim Erhalt der Telefonrechnung.

Apps sollte man grundsätzlich nur in den offiziellen Appstores herunterladen. Es empfiehlt sich auch, immer die Kommentare und Bewertungen anderer User zu lesen, um vielleicht schon im Vorfeld auf einen Betrug aufmerksam zu werden. Darüber hinaus sollte man es sich zur Gewohnheit machen, die Handyrechnung auf irreguläre Kosten zu überprüfen.

Wer auf Nummer Sicher gehen will, kann beim Provider beantragen, dass Mehrwertdienstnummern auf dem Telefon von vornherein gesperrt werden.

Angriff auf ein entsorgtes Smartphone

Sie entsorgen Ihr altes Handy, weil es entweder nicht mehr richtig funktioniert, oder Sie ein neues haben wollen. Kurze Zeit später werden Sie Opfer einer Betrugsmasche, die nur funktionieren konnte, weil die Angreifer Ihre noch auf dem alten Handy befindlichen Daten missbraucht haben.

Handys sind heutzutage richtige Computer, die eine Menge Daten beherbergen. Je nachdem, für welche Dienste das Smartphone genutzt wird, und wie gut es vor der Entsorgung „gereinigt" wurde, lassen sich von einem Hacker so z.B. E-Banking-Daten, persönliche Informationen, Zugangsdaten zu Internetanwendungen und Fotos reproduzieren.

Entnehmen Sie vor dem Entsorgung die SIM- und eventuelle Speicherkarten. Schlagen Sie im Handbuch Ihres Geräts nach, wie Sie Daten endgültig löschen können. Wenn Sie Ihr Handy nicht weiterverkaufen, sondern wegwerfen, können Sie es vorher einfach zerstören.

Spy- und Malware-Angriffe

Smartphones sind nicht immun gegen Schadprogramme. So kann ein Angreifer z.B. Verbindungsdaten oder auch Kreditkartennummern stehlen, indem er dem Smartphone-Benutzer schädliche Apps oder Anhänge in Nachrichten unterjubelt, die auf den ersten Blick nicht als solche zu erkennen sind. Wurde eine Spionagesoftware auf Ihrem Handy installiert, kann diese einen Großteil Ihrer Daten ablesen oder sogar ändern. Des Weiteren gibt es Schadprogramme, die unbemerkt Anrufe an überteuerte Rufnummern tätigen, bzw. Premium-SMS verschicken.

Halten Sie Ihr Handy-Betriebssystem immer auf dem neusten Stand. Laden Sie nur Apps aus den offiziellen Stores herunter. Überprüfen Sie Ihre Telefonabrechnung auf irreguläre Kosten. Öffnen Sie nicht unbedacht Dateien, die Sie auf das Handy geschickt bekommen, auch wenn Sie den Absender kennen. Greifen Sie für Online-Shopping und E-Banking nur auf vertrauenswürdige Anwendungen zurück.

„Network Spoofing“ (verseuchtes WiFi)

Sie sind in der Hotellobby und wollen sich schnell noch ein Zugticket online kaufen. Praktisch, dass das Hotel WiFi anbietet. Schnell ist das Signal gefunden: „Palace_hotel1“ hört sich doch richtig an. Ein Passwort wird nicht verlangt…

Jemand mit kriminellen Absichten kann einen WiFi- oder GSM-Hotspot einrichten, der wie ein legitimes Netzwerk aussieht, um ahnungslose Benutzer dazu zu verleiten, Ihr Gerät damit zu verbinden. Anschließend kann er alle Daten abfangen, die zwischen dem Zugriffspunkt und den Smartphones der Benutzer zirkulieren. Diese Daten kann er später dazu verwenden, gezielte Angriffe, wie zum Beispiel Phishing-Attacken, durchzuführen.

Wenn Sie über öffentliche oder ungesicherte Netzwerke ins Internet gehen, dann vermeiden Sie den Besuch von Seiten, die eine Identifikation (Login) oder die Eingabe persönlicher Daten verlangen. Deaktivieren Sie die automatische Netzwerkverbindung und auch Ihre WiFi-Verbindung, wenn Sie sie nicht benutzen.

Fragen Sie in Restaurants, Hotels, Cafés usw. ob WiFi verfügbar ist, und wenn ja, wie es heißt, beziehungsweise wie das Passwort lautet. Nur WiFi-Netzwerke, die gesichert sind, und ein regelmäßig wechselndes und starkes Passwort haben, sind einigermaßen sicher.

Sollten Sie Fragen zum Thema Online-Betrug oder zur Internetnutzung generell haben, kontaktieren Sie die BEE SECURE Helpline:

BEE SECURE HELPLINE
BERATUNG & HILFE
8002-1234

Union Luxembourgeoise des Consommateurs (ULC)

Wenn Sie online bei einem in Luxemburg ansässigen Unternehmen einkaufen und sich über Ihre Rechte informieren oder über einen Betrug beschweren möchten, kontaktieren Sie die ULC.

www.ulc.lu

Centre Européen des Consommateurs (CEC)

Wenn Sie online in einem anderen Land der EU einkaufen und sich über Ihre Rechte informieren oder über einen Betrug beschweren möchten, kontaktieren Sie das CEC.

Tel. 26 84 64-1 www.cecluxembourg.lu

Institut Luxembourgeois de Régulation (ILR)

Wenn Sie bei Ihrem Telekommunikationsanbieter eine Beschwerde eingereicht haben, können Sie sich, bei einer nicht zufriedenstellenden Lösung des Problems, kostenfrei an die Schlichtungsstelle des ILR wenden.

www.ilr.lu/consommateurs

Police Grand-Ducale

Sie wollen Anzeige wegen Betrugs erstatten?

Schreiben Sie eine E-Mail an contact@police.etat.lu und informieren Sie sich über die genaue Prozedur.

www.police.lu

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+352) 247-86427 · Fax.: (+ 352) 46 41 86
bee-secure@snj.lu · www.bee-secure.lu

Co-funded by the European Union