Kennen Sie diese 11 Hacker-Tricks

Englisches Original von Hackernoon.com

1. **Kopieren und Einfügen (copy paste**)
   Ein kleines Programm (z.B. CryptoShuffler) ändert den Adresscode beim Einfügen und leitet die Coins an eine andere Adresse.
   => Immer die Adresse nach dem Einfügen nochmals kontrollieren !
   => keine unbekannten kostenlosen Apps installieren !
   => regelmäßig Anti-Malware-Programme anwenden

2. **Fake Trading Apps**
   Kostenlose mobile Apps geben vor, günstig und sicher auf Exchanges zu traden, doch der mögliche Handel findet nicht auf einer offiziellen Börse statt, sondern zu Gunsten des Hackers
   => auch auf Mobilephones immer Anti-Malware-Programme laufen lassen !

3. **Slack Channel Hacking Bots**
   Bots, die Alarm bezüglich eines Wallets auslösen, sind Fake. Sie bieten eine Internet-Adresse (URL) an und fragen nach dem Private Key.
   => ignorieren und NIEMALS einen Private Key herausgeben !

4. **Browser-Erweiterungen**
   Browser-Extensions or PlugIns, die verbesserten Krypto-Exchange-Handel anbieten, lesen in Wahrheit alles mit, was über die Tastatur eingegeben wird.
   => auf Extensions am besten verzichten und im Private Mode bleiben !

5. **Geclonte Websites / URLs**
   Externe Links oder Veränderungen in der URL-Eingabe im Browser führen zu gefälschten Webseiten. Deren Name ist oft dem Original

sehr ähnlich, genauso wie das Erscheinungsbild der Website.
=> Eingabe kontrollieren und auf sichere Seiten (möglichst https) achten; URLs genau vergleichen
=> nicht auf externe Links klicken, nur weil diese gerade mit Lockangeboten angepriesen werden
=> wichtige und korrekte Adresse in der Favoritenliste des eigenen Browsers ablegen und von dort aus aufrufen

6. **Gehacktes Google Ranking**
   Hacker verändern das Google Ranking mit ähnlich lautenden Namen und URLs, so dass diese unter den ersten Plätzen erscheinen.
   => nicht blind die ersten Resultate anklicken, sondern immer prüfen !

7. **Social Media Icons**
   Sehr beliebt ist die Nutzung von Social Media Icons von Twitter oder Facebook, bei deren Klick man auf eine Hackerseite geleitet wird.
   => nichts Unbekanntes einfach anklicken, immer die Adresse prüfen. Im Zweifel die Seite umgehend verlassen und vor allem nichts herunterladen, auch keine Bilder.

8. **2FA via SMS**
   Bei vielen Registrierungen wird legitim nach Mobil-Telefonnummern gefragt. Wenn damit aber das Angebot verbunden ist, die Zwei-Faktoren-Authentifizierung (2FA) durchzuführen, ist etwas faul.
   => niemals 2FA via SMS durchführen !

9. **Email-Phishing**
   Emails, die zwar genauso aussehen, wie die von gewohnten und vertrauten Websites, können Fakes sein und nur dem Phishing von Daten dienen. Oftmals ist keine Absenderadresse zu finden, auch keine (Deine) Empfängeradresse, oder es handelt sich um irgendwelche Fantasieadressen.

=> immer Absender- und Empfängeradresse kontrollieren !

=> niemals vertrauenswürdige Daten eingeben !

Merke: kein seriöser Absender fragt nach privaten Daten via Email !

10. Ungeschütztes Wifi

Hackern gelingt es mittlerweile auch Wifi-Router auszuspionieren. Aber besonders einfach ist der Datenklau natürlich in öffentlichen ungeschützten Wifi-Netzen, z.B. in Flughäfen.

=> öffentliche Netze möglichst meiden, in jedem Falle aber keine privaten Daten verwenden und nicht traden !

11. Airdrops

Airdrops sind eine neue Art, kostenlos und einfach an Kryptowährungen zu kommen. Das Versprechen eines Airdrops kann natürlich leicht genutzt werden, um an private Schlüssel zu gelangen.

=> auch hier gilt, NIEMALS den Private Key bekannt geben. Seriöse Anbieter fragen nicht danach !

=> nicht spontan auf jedes Angebot herein fallen. Es muss ausreichend Zeit sein, sich gründlich zu informieren und die Seriosität zu prüfen.