Google QR-Scanner

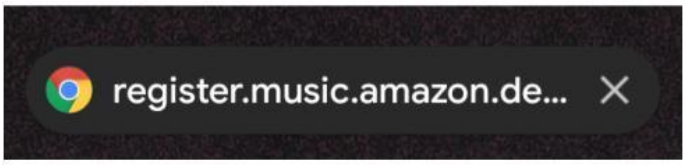
Phishing war und ist noch immer eine Gefahr für alle Internetnutzer:innen. Neben der Vorteile die neue Technologien mit sich bringen, können Betrüger:innen diese ebenfalls für neue Angriffstrategien nutzen. Betrüger:innen versuchen eine betrügerische URL ähnlich wie eine legitime URL aussehen zu lassen. URLs werden zunehmend auch in QR Codes angeboten bzw. verteilt. Auch diese können entsprechend für QR Phishing Angriffe genutzt werden. Google, sowie die meisten anderen Smartphone-Hersteller haben eine eigene QR-Scanner App auf dem Smartphone vorinstalliert. In den App-Stores stehen weitere QR-Scanner zur Verfügung.

Die Frage, die wir uns gestellt haben, ist in wie weit QR-Scanner Nutzer:innen ermöglichen, die ganze URL anzusehen bzw. falls das nicht der Fall ist die wichtigen Teile der URL (sprich vor allem Domain und Top-Level-Domain) anzeigen zu lassen.

Im Rahmen der Untersuchung sind wir über ein signifikantes Problem beim Google Pixel integrierten QR-Reader gestoßen: Die App zeigt den Nutzern:innen die URL von links nach rechts an. Diese Darstellung ergibt auf den ersten Blick Sinn, bis zu dem Punkt an dem die URL eine gewisse Länge erreicht. Wenn die URL zu lang für den Darstellungsbereich ist, wird dieser von dem QR-Scanner abgeschnitten und kann im schlechtesten Fall nur die Subdomains anzeigen.

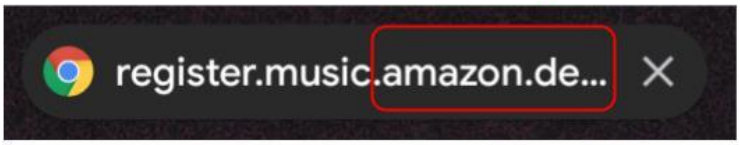
In dem folgenden Beispiel demonstieren wir die an einem Google Pixel 5 mit Android Version 12. Um dies zu verdeutlichen, haben wir Domain+Top-Level-Domain in rot hervorgehoben. Es ist wichtig zu erwähnen, dass die verwendete Webseite nicht real ist, lediglich stellt die Hauptdomain (Amazon) ein reales Unternehmen dar, welches nichts mit dem Problem des QR-Scanners zu tun hat.

Potential Legitimate Link:
https://register.music.amazon.de/eeee



Potential Phishing Link:
https://register.music.amazon.de.phishme.com/eeee

Android 12



Android 13

Die Anzeige ist in beiden Fällen, legitim und betrügerisch, identisch. Da es keinerlei Option gibt die URL in voller Länge zu betrachten, ist es für die Nutzer:innen in diesem Fall unmöglich zu unterscheiden, ob die gezeigte URL legitim oder betrügerisch ist.

Nach erfolgreicher Kontaktaufnahme mit Google als auch dem BSI, wurde das Problem mit dem neusten Android Update behoben, dass nun jederzeit die Domain mit Top-Level-Domain angezeigt wird. Dies zeigt auch wieder, wie wichtig es ist, die eigenen Geräte upzudaten, um jederzeit die neusten Sicherheitsstandards zu erhalten.