Fünf Beispiele wie Mitarbeiter über mobile Geräte Opfer von Phishing werden

Mobile Geräte sind jetzt der einfachste Weg, Unternehmensdaten zu kompromittieren

Ihre Mitarbeiter wissen, wie sie Phishing-Versuche auf PCs erkennen können, aber auf mobilen Geräten wie Smartphones oder Tablets ist das viel schwieriger. Es gibt zahlreiche Kanäle, um Nutzer mobiler Geräte mit Social Engineering Angriffen zu täuschen.

1. SMS und iMessage

2. Messaging-Apps von Drittanbietern

3. Plattformen sozialer Medien

4. E-Mail- und Produktivitäts-Suiten

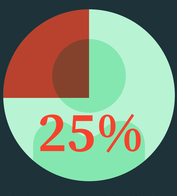
5. QR-Codes

4.000.000

mobile Phishing-Angriffe wurden im Jahr 2023 von Lookout verhindert

Ein erfolgreicher Phishing-Angriff gewährt den Angreifern Zugang zu allen Informationen.

Mitarbeiteridentitäten sind das Einfallstor zu in der Cloud gespeicherten Daten. Bedrohungsakteure haben es auf mobile Geräte abgesehen, um Anmeldeinformationen zu stehlen, MFA-Lösungen zu umgehen und sich unbemerkt Zugang zu Ihren Daten zu verschaffen.



der Nutzer von mobilen Geräten waren 2023 mehrfach von Phishing-Angriffen betroffen

der Mitarbeiter in Unternehmen haben im Jahr 2023 mindestens sechs Phishing-Links angeklickt

Bei mobilen Phishing-Angriffen werden nicht nur Anmeldedaten gestohlen.

Viele bösartige Websites versuchen, Anmeldedaten zu stehlen. Andere übertragen Malware oder nutzen eine Sicherheitslücke aus, um Zugang zum Gerät selbst zu erhalten. Manche tun sogar beides.

48%

der bösartigen Websites zielen auf die Verbreitung von Malware oder die Ausnutzung von Sicherheitslücken ab.

Aktuelle Bedrohung: CryptoChameleon

Das Lookout Research Team hat ein fortschrittliches Phishing-Kit entdeckt, das neuartige Taktiken aufweist, um Behörden und Unternehmen über mobile Geräte anzugreifen. Dieses Kit ermöglicht es Angreifern:

- Kopien von Single Sign-On (SSO)-Seiten zu erstellen
- Eine Kombination aus E-Mail-, SMS- und Voice-Phishing zu verwenden, um Zielpersonen zu täuschen
- Benutzernamen, Kennwörter, URLs zum Zurücksetzen von Kennwörtern und Foto-IDs zu stehlen.

Um mehr über CryptoChameleon und ähnliche Bedrohungen zu erfahren, besuchen Sie das Lookout Threat Lab.