



Smishing

Beim Smishing versenden Betrüger Textnachrichten, um beispielsweise sensible Daten abzugreifen oder Schadsoftware zu verbreiten. Der Begriff setzt sich aus „SMS“ und der verwandten Betrugsmasche „Phishing“ zusammen.

Datenklau per SMS

Smishing ist eine auf Kurznachrichten zugeschnittene Variante des traditionellen E-Mail-Phishing. Dabei sollen die eingehenden SMS beim Nutzer den Anschein erwecken, von einer vertrauenswürdigen Person oder Organisation zu stammen. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) wollen sich die Hacker auf diese Weise hauptsächlich den Zugang zu Bankkonten ergattern: Beim sogenannten „Bank Smishing“ verschicken die Täter Nachrichten, die vermeintlich von der Bank des Opfers stammen. Die SMS warnen ihren Empfänger vor unrechtmäßigen Abbuchungen oder unbekannten Zahlungsempfängern und stellen einen Link zur Verfügung, um den bevorstehenden Zugriff auf das Bankkonto zu verhindern. Dieser führt in der Regel auf eine gefälschte Webseite. Ziel ist es, das Opfer dazu zu bewegen, seinen Nutzernamen und sein Passwort preiszugeben, um im Anschluss das Konto plündern zu können. Bei einer anderen Variante von Smishing versuchen Kriminelle ihre Opfer dazu zu verleiten, gefährliche Malware (z. B. Trojaner) auf ihrem Mobiltelefon zu installieren, um beispielsweise deren Kreditkarteninformationen abzugreifen oder andere App-Zugangsdaten zu kompromittieren. So gehen in letzter Zeit auf immer mehr Mobiltelefonen SMS zur Sendungsnachverfolgung von Paketen ein, über die der Banking-Trojaner FluBot installiert wird. Gängige Formulierungen in Phishing-SMS sind z. B. „Ihr Paket wird bald geliefert. Zur Sendungsverfolgung klicken Sie auf diesen [LINK]“ oder „Sehr geehrter Sparkassen Kunde, ihr TAN-Verfahren ist abgelaufen! Bitte erneuern Sie Ihr TAN-Verfahren direkt unter: [LINK]“.

Warnzeichen und Schutz

Anhand folgender Merkmale lässt sich eine Phishing-SMS erkennen:

In der SMS befinden sich Rechtschreibfehler oder falsche Grammatik.

Der Nutzer wird aufgefordert, persönliche Daten einzugeben.

Der Absender klingt verdächtig/unseriös oder enthält kryptische Zahlen- und Buchstabenkombinationen.

Die SMS enthält einen Link zur Sendungsverfolgung, obwohl keine Bestellung aufgegeben wurde.

Beim Erhalt einer verdächtigen SMS rät das BSI, keinesfalls auf den Link zu klicken, die Nachricht umgehend nach Erhalt zu löschen und den Absender über das Betriebssystem zu sperren. Grundsätzlich sollte unter Android die Installation von Apps aus unbekannten Quellen deaktiviert werden. Über den Mobilfunkanbieter lässt sich außerdem eine sogenannte Drittanbietersperre aktivieren, um unerwünschte Abbuchungen zu vermeiden. Nutzer, die bereits auf einen einschlägigen Link geklickt oder schädliche Software installiert haben, sollten ihr Gerät in den Flugmodus schalten und so vom Mobilfunknetz trennen. Im Anschluss sollte man den Provider über den Fall informieren sowie das Bankkonto auf nicht selbst veranlasste Abbuchungen überprüfen. Darüber hinaus empfiehlt das BSI, Strafanzeige bei der örtlichen Polizeidienststelle zu erstatten.

KF (Stand 30.04.2021)

Siehe auch:

[Phishing](#)

[Malware/Spyware](#)

[Cybercrime](#)

