SOPHOS
Cybersecurity made simple.

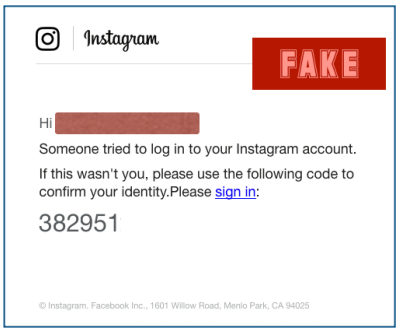
Phishing-Attacke für Instagram-Account nutzt 2FA-Köder

Exzellent vorbereitet, absolut glaubwürdig und vermutlich sehr effizient – SophosLabs ist ein besonders intriganter Fall von Phishing ins Netz gegangen. Eine Analyse der Attacke auf Instagram-Nutzer und eine Erinnerung an bewährte Sicherheitstipps.

Als Cyberkriminelle das erste Mal Phishing in großem Stil einsetzten, gingen sie direkt dorthin, wo sie Geld vermuteten: zum Bankkonto. In Folge erhalten Nutzer bis heute Warnmeldungen von Banken, mit denen sie noch nie zu tun hatten. Ominöse Experten empfehlen mit schlechter Grammatik und kurioser Rechtschreibung auf noch merkwürdigere Webseiten zu gehen. Achtsamkeit ist also ein guter Rat, bis heute. Denn die meisten Betrüger machen Fehler, die sie entlarven. Schlimm genug, überhaupt Opfer eines Phishing-Angriffs zu werden. Aber es ist noch viel ärgerlicher, wenn man sich aus Unachtsamkeit bei der „Deutschenn Bank“ oder der „Volcksbank“ einloggt.

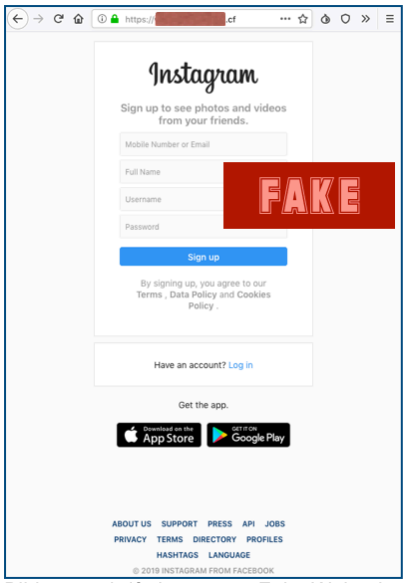
Besonders wertvoll: Passwörter für Instagram, Facebook und Co.
Heutzutage sind nach wie vor Phishing-E-Mails im Umlauf, die versuchen, Bank-Zugangsdaten zu erbeuten. Hinzukommen aber zahlreiche Phishing-Mails, die nach weiteren Account-Passwörtern trachten. E-Mail-Konten etwa sind der Hauptgewinn für Betrüger. Sie dienen häufig als Referenzadresse zur Wiederherstellung vergessener Passwörter. Gelangt ein Cyberkrimineller an einen E-Mail-Account, kann er damit diverse andere Konten (Paypal, Facebook, Instagram etc.) ins Visier nehmen und sich über die Funktion „Passwort zurücksetzen“ oder „Passwort vergessen“ dauerhaften Zugang zu vielen anderen Accounts zu verschaffen. Besonders gemein: das Opfer merkt davon meist gar nichts. Bis etwas passiert, natürlich.
Aber auch Passwörter für soziale Medien sind für Betrüger ein beliebtes Ziel. Denn die Inhalte dieser Konten offenbaren den Kriminellen weit mehr Informationen als sie mit regulärer Recherche je erfahren könnten. Dabei sind die Folgen mehrfach gemein: sie sind sehr persönlicher Natur und sie treffen zudem Dritte. So vermag der Betrüger beispielsweise auch den Account von Freunden oder Familienmitgliedern zu manipulieren.
Tatsächlich überwiegen bereits heute Phishing-Mails, die nach Passwörtern für E-Mail- und Social-Media-Accounts trachten, gegenüber denen, die hinter Bankzugängen her sind.

Die Betrüger werden immer besser – ein „exzellentes“ Beispiel
Es fällt schwer es zuzugeben, aber die Betrüger arbeiten mittlerweile gut und überlegt, wie folgendes Beispiel zeigt:
Abgesehen von wenigen Interpunktionsfehlern und einem fehlenden Leerzeichen vor dem „Please“, ist diese Nachricht kaum als Fake zu erkennen. Sie ist klar und unauffällig genug, um unterhalb des menschlichen Alarmradars zu bleiben. Die Verwendung der Zahlenreihe, die auf den ersten Blick wie ein 2FA-Code erscheint, ist ein cleverer Schachzug. Die Verwendung impliziert, dass der Nutzer kein Passwort verwenden muss, sondern stattdessen einfach nur per Code bestätigen muss, dass ihn die E-Mail erreicht hat. Der 2FA-Code täuscht Sicherheit vor.



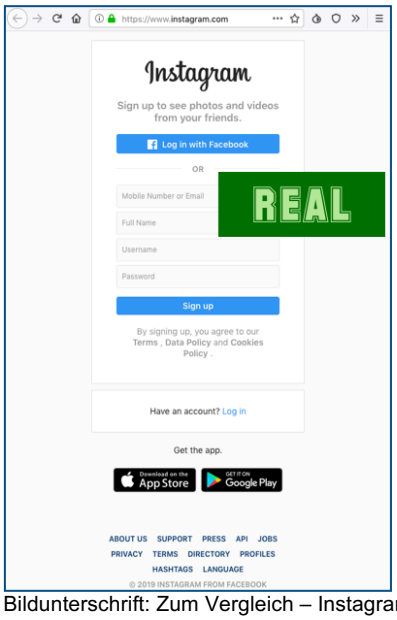
Bildunterschrift: Instagram Phishing-Mail

Klickt man in der Mail auf den Link, könnte man im Browser am Domainnamen (hier im Beispiel unkenntlich gemacht) den Betrugsversuch erkennen oder zumindest vermuten. Es ist eine Seite mit Domain-Endung „cf“ für Centralfrique, eine der vielen aufstrebenden Volkswirtschaften, die Domains für wenig Geld vergeben in der Hoffnung, möglichst viele User mit möglichst cool klingenden Domain-Namen zu ködern.



Bildunterschrift: Instagram Fake Webseite

Experten der SophosLabs gehen davon aus, dass die Betrüger gezwungen waren, eine der frei verfügbaren, aber eben doch etwas weniger glaubwürdigen Domainnamen zu nutzen. Dennoch ist diese Phishing-Seite ein nahezu perfekter und glaubwürdiger Nachbau der echten Seite und verfügt sogar über ein valides HTTPS-Zertifikat.



Bildunterschrift: Zum Vergleich – Instagram Original-Webseite

Michael Veit, Security Experte bei Sophos, erklärt: „Web-Zertifikate sichern eine Verbindung zu einer Website und verhindern, dass Antworten angeschaut oder manipuliert werden können. Sie sorgen dafür, dass die Person, die das Zertifikat erworben hat, sich wirklich an der Website anmeldet und diese auch ändern kann. Die Zertifikate bürgen jedoch nicht für den tatsächlichen Inhalt der Webseiten oder dort verfügbare Dateien. Mit anderen Worten: einer Website ohne Vorhängeschloss ist definitiv nicht zu trauen, ebenso wenig wie einer mit Tipp- und Grammatikfehlern. Doch auch bei Webseiten mit „Vorhängeschloss“ und scheinbar fehlerfreier Umsetzung gilt grundsätzlich immer, Vorsicht walten zu lassen.“

Prävention ist wichtig
Wie macht sich eine Phishing-Seite, die glaubhaft wirkt und ein HTTPS-Vorhängeschloss mitbringt, verdächtig? Michael Veit sagt: “Obwohl die Betrüger in diesem Beispiel einen ungewöhnlich glaubwürdigen Fake kreiert haben, gibt es verräterische Anzeichen von Phishing-Attacken, an denen man sich orientieren kann.“

Drei Tipps für das Erkennen von Phishing-Aktivitäten:

- **Sign-in Links in E-Mails.** Die einfache Lösung: ab in den Papierkorb. Warum sollte man sich via E-Mail in einen seiner Social-Media-Accounts einloggen? Das geht doch direkt. Wahlweise via App oder Lesezeichen im Browser anmelden.
- **Überraschender Domainname.** Wo hat der Browser mich hingeführt? Ist die Adresszeile zu kurz für die komplette URL? Ein einfacher Trick: die Adresszeile kopieren und in ein anderes Dokument einfügen. Sieht verdächtig aus? Dann ist sie es wohl auch. Besser ignorieren oder eine zweite Meinung dazu einholen.
- **Anfrage ohne Grund.** Besteht Grund zur Annahme, ein Fremder hätte sich in den eigenen Account eingeloggt, sollten Nutzer zur Prüfung der Login-Aktivitäten die offiziellen Möglichkeiten des Dienstanbieters wählen. Es gibt keinen Grund, Web-Links zu trauen, die von irgendwo kommen könnten. Ärgerlicherweise gibt es kein einheitliches Verfahren bei den verschiedenen Social-Media-Apps. Aber mit etwas gesundem Menschenverstand und Übung können betrügerische Prozesse schnell erkannt werden.

Die Grafiken stehen zum Download bereit unter:
https://presselounge.tc-communications.de/sophos.html

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de