

t3n.de

Von Smishing bis Whaling: 9 Arten von Phishing-Angriffen, die ihr kennen solltet - t3n – digital pioneers

Marvin Fuhrmann

10–12 Minuten

Egal, ob für Privatpersonen oder Unternehmen: Phishing-Angriffe stellen ein hohes Risiko für Daten dar. Laut dem [BSI](#) ist Phishing nach wie vor die größte digitale Bedrohung für viele Menschen. Die [Cybersecurity & Infrastructure Security Agency](#) in den USA geht sogar davon aus, dass 90 Prozent aller erfolgreichen Cyberangriffe mit einer Phishing-Attacke beginnen.

- [E-Mail-Phishing](#)
- [Spear-Phishing](#)
- [Whaling](#)
- [Vishing](#)
- [Smishing](#)
- [Clone-Phishing](#)
- [Angler-Phishing](#)
- [Pharming](#)
- [Evil-Twin-Phishing](#)

Beim Phishing werden Personen online von Cyberkriminellen kontaktiert. Diese geben dabei vor, ein wichtiger Kontakt oder ein Unternehmen zu sein, mit dem die Personen zu tun haben. Das kann von engen Freunde über Vorgesetzte hin zu Banken und Online-Händler reichen. Ziel der Phishing-Nachrichten ist es, eine möglichst dringliche Situation vorzutäuschen und dementsprechend schnelles Handeln von den Personen zu erzwingen. In der Eile sollen sie dann sensible Daten eingeben und übersenden.

Diese Daten landen bei den Cyberkriminellen. So verschaffen sie sich Zugriff auf Konten, Mail-Postfächer oder sogar auf interne Strukturen von Unternehmen. Mittlerweile haben sich Cyberkriminelle einige Mittel und Wege einfallen lassen, um uns zu täuschen. Wir verraten euch die wichtigsten Phishing-Arten, damit ihr euch besser davor schützen könnt. Weitere Tipps, wie ihr [Phishing-Mails erkennt und wer bei Schaden haftet](#), verraten wir euch im verlinkten Ratgeber.

E-Mail-Phishing

Der Klassiker unter den Phishing-Angriffen nimmt eine breite Masse von Internetnutzern ins Visier. Cyberkriminelle verschicken [Nachrichten im Namen von verschiedenen Organisationen](#) an Mail-Adressen, die sie oftmals im Darknet gekauft haben. Die Adressen landen dort häufig durch Leaks oder Hacking-Angriffe. In den Nachrichten wird etwa behauptet, dass euer Bankkonto oder Account bei einem Unternehmen gesperrt wurde.

Empfehlungen der Redaktion

↻ Artikel wechseln

Um es zu entsperren, müsst ihr nur sensible Daten in ein Formular eingeben. Cyberangreifer verschleiern dabei oftmals ihre Mail-Adresse, um den Empfängern vorzugaukeln, dass es sich um eine echte Nachricht des Unternehmens handeln würde. Oftmals reicht es schon aus, nicht auf die Mail zu antworten und euch in das zugehörige Konto einzuloggen. Gibt es dort keine sichtbaren Probleme, könnt ihr noch beim Support nachfragen. Oftmals wissen die Mitarbeiter schon Bescheid, dass es vermehrt zu Phishing-Angriffen per Mail kommt – und können euch Entwarnung geben.

Spear-Phishing

Das Spear-Phishing funktioniert im Grunde wie klassisches Phishing. Der Unterschied ist, dass die Cyberkriminellen nur eine besonders kleine Gruppe von Menschen ins Visier nehmen. Das können etwa alle Mitarbeiter eines Unternehmens oder nur bestimmte Abteilungen wie IT-Angestellte sein. Die Angreifer zielen dabei oftmals auf sensible Daten aus dem Unternehmen ab – oder Zugriff auf ganze Systeme.

Whaling

Whaling ist noch einmal eine etwas präzisere Variante von Spear-Phishing. Statt eine bestimmte Gruppe in einer Organisation zu kontaktieren, greifen die Cyberkriminellen gezielt die wichtigsten Personen an. Dazu zählen dann etwa CEOs oder andere Mitarbeiter mit Zugriff auf alle Daten des Unternehmens. Sollte ein Whaling-Angriff erfolgreich sein, folgen darauf häufig weitere Angriffe. Denn mit Zugriff auf das Mail-Postfach eines CEOs können die Angreifer das [ganze Unternehmen mit echt](#)

[aussehenden Phishing-Mails torpedieren.](#)

Von sinnfreien Sicherheitsfragen bis zu unsicheren Passwörtern:
Die dümmsten Security-Patzer

Vishing

Vishing ist ebenfalls eine Unterart der Phishing-Angriffe, unterscheidet sich aber primär durch die Plattform des Angriffs. Denn im Unterschied zu E-Mail-Angriffen werden potenzielle Ziele von den Cyberkriminellen angerufen. Der Name Vishing ist eine Kombination aus Phishing und Voice. Dabei können die Angreifer ebenfalls vorgeben, dass sie von einem Unternehmen wie Microsoft stammen und es angeblich ein Problem mit dem PC der Angerufenen geben würde. Auch Anrufe von vermeintlichen Bankmitarbeitern sind verbreitet, da diese [Vishing-Angriffe schnell Zugriff auf Kontodaten ermöglichen.](#)

Smishing

Auch das Smishing unterscheidet sich durch die Plattform, auf dem die Phishing-Angriffe stattfinden. Smishing ist eine kürzere Version des Begriffs SMS-Phishing. Dementsprechend werden die betrügerischen Nachrichten über SMS oder Messenger-Dienste wie Whatsapp verschickt. Gerade bei Messengern versuchen die Betrüger dabei oftmals den [Account zu übernehmen, indem sie einen Code von euch verlangen,](#) während sie sich als einer eurer Kontakte ausgeben.

Clone-Phishing

Bei Clone-Phishing haben die Angreifer meist schon Zugriff auf ein

bestimmtes E-Mail-Postfach einer Privatperson oder eines Unternehmens. Damit sie sich keine Nachrichten ausdenken müssen, die besonders echt aussehen, fangen sie einfach echte Mails ab und kopieren diese. Während das Original gelöscht wird, verändern sie in der Kopie etwa nur einen Link. So könnte etwa eine Mail von euren Kollegen eintreffen, die sich um den aktuellen Quartalsbericht dreht. Im Anhang wurde ein Link zu einem Google-Doc hinterlegt. Der schädliche Link führt dann aber nicht zu dem Doc, sondern zu einer Seite, die eure Login-Daten abgreift oder Schadsoftware herunterlädt.

Sinnvolle und weniger sinnvolle Tipps für Passwörter

Angler-Phishing

Angler-Phishing macht sich Social-Media-Plattformen zunutze. Cyberkriminelle erstellen Fake-Konten, die denen von bekannten Unternehmen oder Prominenten nachempfunden sind. Sie treten dann in [direkten Kontakt mit Privatpersonen](#), antworten auf ihre Kommentare oder liken ihre Beiträge. So schaffen sie Vertrauen. Das kann besonders dann Schaden anrichten, wenn die Angreifer sich als Kunden-Support ausgeben. Sie schicken dann Links zu vermeintlichen Support-Webseiten mit Lösungsansätzen. Tatsächlich fangen sie darüber entweder sensible Daten ab oder infizieren die Geräte der Ziele mit Schadsoftware.


Pharming

Beim Pharming manipulieren die Angreifer den Zugriff auf Webseiten. Um das zu erreichen, wurde oftmals auf anderem Wege Malware auf das Endgerät der Ziele geladen. Beim Aufrufen

von Webseiten manipuliert die Schadsoftware dann die Weiterleitung und führt die Nutzer auf Fake-Seiten. Sämtliche Daten, die dann von den Nutzern auf der Seite eingegeben werden, landen bei den Cyberkriminellen.

Evil-Twin-Phishing

Der böse Zwilling beim Evil-Twin-Phishing ist die [Kopie eines Wi-Fi-Zugangs](#). Befindet ihr euch etwa in einem Café mit einem öffentlichen WLAN, können Angreifer einen Hotspot auf ihrem Endgerät erstellen und diesen ähnlich benennen. Oftmals sind die Hotspots im Vergleich zu den richtigen Zugangspunkten nicht geschützt, sodass sich Nutzer ohne Hindernisse einloggen können. Durch die direkte Verbindung zu den Geräten der Hacker können zahlreiche Daten von euren Geräten gestohlen werden.

Verpasse keine News zu Software & Entwicklung 

Bitte gib eine gültige E-Mail-Adresse ein.

Es gab leider ein Problem beim Absenden des Formulars. Bitte versuche es erneut.

Bitte gib eine gültige E-Mail-Adresse ein.

[Hinweis zum Newsletter & Datenschutz](#)