# WIE MOBILES PHISHING FUNKTIONIERT UND WAS MAN DAGEGEN TUN KANN

APWG

EIN BERICHT DER ANTI-PHISHING WORKING GROUP (APWG)

# EINFÜHRUNG

Mobile Geräte sind zu einem festen Bestandteil des Privat- und Geschäftslebens geworden und erfordern fast jede Minute Tag und Nacht unsere Aufmerksamkeit. Diese Allgegenwart, gepaart mit den Einschränkungen eines kleinen Bildschirms sowie begrenzter Speicher- und Rechenleistung, bedeutet jedoch, dass mobile Geräte oft weniger gegen Sicherheitsbedrohungen geschützt sind als PCs oder Laptops. Erschwerend kommt hinzu, dass viele Mitarbeiter von Unternehmen ihre persönlichen Mobilgeräte für geschäftliche Zwecke nutzen.

In diesem Bericht der Anti-Phishing Working Group (APWG.org) werden zahlreiche Phishing-Bedrohungen beschrieben, die Benutzer von mobilen Geräten betreffen. Außerdem werden die besonderen Herausforderungen bei der Abwehr von mobilen Bedrohungen und der Schutz von Desktop-Endgeräten im Unternehmensumfeld behandelt. Abschließend wird ein Weg sowie mehrere bewährte Methoden zum Schutz von mobilen Geräten und Benutzern vor verschiedenen Arten von Phishing- und Spear-Phishing-Angriffen und neuartiger Bedrohungsvektoren wie Sprache und SMS beschrieben.

# 2018 WAR DAS JAHR DES „PHISH“

Es ist nicht überraschend, dass Phishing eine der größten Herausforderungen für Sicherheitsteams ist. Ein falscher Klick eines unbedarften oder unzureichend ausgebildeten Mitarbeiters könnte schließlich das Unternehmensnetzwerk, die Website, Backend-Systeme oder das gesamte Unternehmen ausschalten. In der Folge können Hacker Netzwerke mittels Advanced Persistent Threats (APTs) infiltrieren und Spear-Phishing-Angriffe auf Corporate Controller ausführen, um erhebliche Summen Geldes zu stehlen und sich Zugriff auf die Anmeldeinformationen zu verschaffen. Auf diese Weise können fachkundige Eindringlinge laterale Angriffe auf das gesamte Unternehmen starten. Diese Angriffe können im schlimmsten Fall auf nationaler Ebene erfolgen.

Die durch Phishing-Attacken verursachten finanziellen Einbußen und Reputationsschäden sowie gesetzliche Risiken und Geldbußen bei Nichtbeachtungkönnen enorm sein. Beispielsweise ergab eine Studie von Ponemon aus dem Jahr 2018 über die Kosten von Datenpannen – der Goldstandard der Branche im Bereich Studien –, dass die durchschnittlichen weltweiten Kosten einer Datenpanne bei 3,86 Millionen US-Dollar den Wert des Vorjahres um 6,4 % überstiegen.

## Hochmoderne Phishing-Kunst

Phishing ist nichts Neues. Im Grunde handelt es sich um eine bewährte Form der Cyberkriminalität, bei der Bedrohungsakteure versuchen, Menschen durch unerwünschte Kontaktaufnahme, etwa per E-Mail oder SMS, dazu zu bewegen, Links zu öffnen oder andere Handlungen durchzuführen, in deren Folge sie Computersysteme infizieren, vertrauliche Informationen stehlen oder andere unlautere Ziele verfolgen. Tatsächlich ist Phishing derart weit verbreitet und effektiv, dass Malware nach Phishing nur noch der zweitgefährlichste Angriffsfaktor ist, gefolgt von gezielten Hackerangriffen gegen ungeschützte oder falsch konfigurierte Systeme.

# ANGRIFFE AUF BENUTZER VON MOBILGERÄTEN

Im Zeitalter des Mobilfunks werden bei Phishing eine Reihe neuer Techniken verwendet, um Anwender dazu zu bewegen, Folgendes zu tun:

- Besuch einer gefälschten Website, durch die Malware auf dem mobilen Gerät des Mitarbeiters installiert wird
- Öffnen eines Anhangs, der schädlichen Code auf dem mobilen Gerät des Mitarbeiters installiert
- Auf gefälschte Anrufe oder Voicemails von falschen Quellen zu reagieren, die sich als Bank des Unternehmens, als legitimer Verkäufer oder Ähnliches ausgeben, um vertrauliche Informationen zu erhalten, insbesondere Kontodaten

## Phishing von mobilen Geräten findet auf mehreren Kanälen


E-Mail

SMS/Text/iMessage


Apps


## E-Mail-Phishing

Mobile Geräte sind besonders schwer gegen E-Mail-Phishing zu schützen, weil:

**Die Bildschirmgröße des mobilen Geräts die Überprüfung von URLs verhindert:** Die Bildschirme für mobile Geräte sind klein. Das genaue Ziel einer an einen Benutzer per E-Mail gesendeten URL zu erkennen, ist auf einem kleinen Bildschirm schwierig oder sogar unmöglich. Eine per E-Mail verschickte URL, die sich als Aufforderung zum Zurücksetzen des Kennworts einer Bank herausstellt, könnte beispielsweise wie folgt aussehen:

www.bankname.com.securityupdate.phishingsite.com

**Die Bildschirme für mobile Geräte sind klein. Das genaue Ziel einer an einen Benutzer per E-Mail gesendeten URL zu erkennen, ist auf einem kleinen Bildschirm schwierig oder sogar unmöglich.**

Bei der Anzeige auf dem kleinen Bildschirm eines E-Mail-Clients oder eines E-Mail-Browsers auf einem mobilen Gerät wird den Benutzern nicht die vollständige URL angezeigt, und sie werden zu der Annahme verleitet, dass sie www.bankname.com besuchen, während Sie in Wirklichkeit eine gefälschte Webseite, die von phishingsite.com kontrolliert wird, aufrufen.

**Geräte verbinden sich mit mehreren E-Mail-Konten:** Mobile Geräte werden häufig für geschäftliche und private Zwecke verwendet. Angesichts der heutzutage breit angelegten Initiativen zu BYOD-Programmen (Bring Your Own Device) bedeutet dies, dass Unternehmen von Mitarbeitern erwarten, dass sie ihre eigenen Geräte für berufliche Aufgaben und E-Mail verwenden.

Die gemischte Verwendung bedeutet somit auch, dass die Geräte sich mit mit mehreren E-Mail-Konten verbinden. Das geschäftliche E-Mail-KOnto wird von vom serverseitigen Spam- und Phishing-Schutz profitieren. Es werden jedoch andere E-Mail-Konten für persönliche E-Mails verwendet, die nicht von den serverseitigen Schutzmaßnahmen des Unternehmens profitieren. Infolgedessen können bösartige Akteure Phishing-E-Mails leicht über diese alternativen E-Mail-Kanäle an Unternehmensbenutzer übermitteln, wodurch jegliche Art von serverseitigem Schutz des Unternehmens umgangen wird.

Da E-Mail-Apps auf mobilen Geräten normalerweise so konfiguriert und verwendet werden, dass alle E-Mails aller verbundenen Konten in einem einzigen einheitlichen Posteingang angezeigt werden, ist es unwahrscheinlich, dass Benutzer erkennen können, an welches Konto eine Phishing-E-Mail gesendet wurde. Dadurch kann Business Email Compromise Phishing (BEC) sowohl private als auch für Unternehmenskonten angreifen.

## E-Mail-Spear-Phishing

Im Jahr 2018 kam es zu einem Anstieg gezielter Phishing-Angriffe, bei denen Informationen aus verschiedenen Quellen herangezogen wurden, um die Empfänger von der Echtheit gefälschter Kommunikation zu überzeugen. Dazu gehörten:

**Spear-Phishing-Angriffe auf Verbraucher:** Bei diesen Betrügereien werden gestohlene Datenbanken mit Namen, Telefonnummern und Konten der Kunden verwendet, um sehr zielgerichtete und überzeugende Nachrichten zu erstellen. Beispielsweise können Hacker eine gestohlene Datenbank mit Anmeldeinformationen eines Markenbetreibers – beispielsweise wie im Fall Equifax oder Yahoo! – verwenden, um Handybenutzern gezielte Nachrichten unter Verwendung des Namens dieser Marke oder der persönlichen Informationen des Empfängers zu senden.

**Spear-Phishing-Angriffe auf Mitarbeiter und Führungskräfte von Unternehmen:** Heutzutage können raffiniertere, finanziell motivierte Angreifer mehr Ressourcen einsetzen, um auf größere Fische zu zielen. Beispielsweise können sie von einem leitenden Mitarbeiter die erforderlichen Zugangsdaten für den Zugang zu Finanzsystemen ausspähen. Diese heimtückischen Angriffe erfolgen gezielt und werden sorgfältig geplant und ausgeführt. Angreifer verwenden in diesen Fällen keine Massenautomatisierung, wie in den zuvor beschriebenen Fällen. Stattdessen spionieren sie Einzelpersonen über Mitarbeiter- und Management-Informationen auf Unternehmenswebsites und Social-Media-Profilen wie LinkedIn, Facebook und Twitter aus und kombinieren diese dann mit Daten aus Online-Datenbanken, die Telefonnummern enthalten.

Darüber hinaus scheinen diese Angriffe häufig von der IT-Abteilung des Unternehmens zu stammen und können Benutzer zu gefälschten URLs weiterleiten, um Passwörter und VPN-Anmeldeinformationen zu erfassen. Sie können auch verwendet werden, um Benutzer zu gefälschten Webseiten des Unternehmens weiterzuleiten, und sie aufzufordern, gefälschte VPN-Profile oder Geräte-Management-Zertifikate des Unternehmens zu installieren.

## SMS-Phishing

SMS-, Text- und iMessage-Phishing, auch bekannt als *Smishing*, ist ein zunehmend verbreiteter Vektor für die Übermittlung schädlicher URLs an Benutzer mobiler Geräte. Laut dem Bericht *2018 State of the Phish™*, wurde Smishing in 2018 bekannt. Der Bericht zeigt, dass die durchschnittliche Fehlerrate bei simulierten Smishing-Angriffen die gleiche ist wie bei E-Mail-Phishing-Tests. Allerdings konnten nur 16 % der weltweit befragten Technologiebenutzer die Definition von Smishing in einer Multiple-Choice-Abfrage korrekt angeben.

Diese Angriffe gibt es in mehreren Varianten:

**Großflächiges Phishing:** Diese Angriffe ähneln E-Mail-Spam-Angriffen, bei denen an tausende Telefonnummern generische Phishing-Nachrichten gesendet werden, die scheinbar von Banken, E-Mail-Anbietern, App-Stores und anderen Online-Diensten stammen. Die Tricks, die bei diesen Angriffen verwendet werden, können das Zurücksetzen von Kennwörtern, Aktualisieren der Kontosicherheit oder sogar falsche Benachrichtigungen über eingehende Zahlungen umfassen, die bestätigt werden müssen.


*Ein Paradebeispiel für einen Smishing-Angriff ist das Stehlen von Bankzugangsdaten*

## App-Phishing

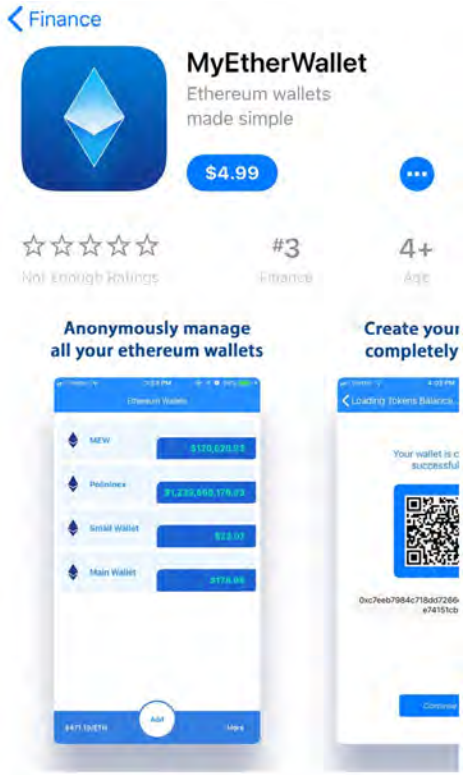
E-Mail und SMS/Text/iMessage sind nicht die einzigen Vektoren, die Phisher zur Übermittlung von Betrugsmeldungen und URLs an Benutzer verwenden. Mobile Apps sind auch zu bedeutenden Kanälen für die Verbreitung von Phishing-Links geworden. Auf den meisten mobilen Geräten ist eine Vielzahl von Apps installiert, und die Anzahl dieser Apps scheint täglich zu steigen. Derzeit sind 3,8 Millionen Apps für Android-Nutzer bei Google Play verfügbar, und über 2 Millionen Apps stehen Benutzern im Apple App Store zur Verfügung. Über 1,5 Millionen Apps sind in App-Stores von Drittanbietern verfügbar, ganz zu schweigen von gefälschten oder bösartigen App-Stores.

### *App-Phishing nimmt außerdem eine Reihe von Formen an:*

**Encrypted Communication Phishing:** WhatsApp, Telegram, Signal und andere Apps liefern verschlüsselte Nachrichten an Benutzer, die nicht gefiltert werden. Sie zählen zu den Hauptkanälen für den Versand von Phishing-Links. Beachten Sie, dass der Absender im Gegensatz zu E-Mails nicht leicht zu fälschen ist. Es können jedoch überzeugende Nachrichten gesendet werden, die vorgeblich vom Kundensupport, vom IT-Support des Unternehmens oder einem bekannten Onlinedienst stammen. Außerdem können diese schädlichen Links nicht vom Unternehmen markiert werden.

**Fake Social Media-Phishing:** Apps wie Twitter sorgen dafür, dass der Benutzer immer mit Social-Media verbunden ist. Diese Apps werden jedoch häufig auch für die Kundenunterstützung von bekannten Bereichen wie Banken, Reisedienstleistern, E-Mail-Anbietern und E-Commerce-Websites verwendet. Angreifer richten auf diesen Social-Media-Seiten Konten ein, die sich als legitimer Kundendienst für diese Unternehmen ausgeben. Über diesen Kanal können sie dann URLs an Benutzer übermitteln und Passwörter oder andere vertrauliche Informationen anfordern.

**Falsche Apps:** Es ist ein weit verbreitetes Missverständnis, dass kommerzielle App-Stores wie der Apple App Store und Google Play nur sichere Apps auf ihren Plattformen zulassen. Jeden Monat schleichen sich eine Vielzahl gefährlicher oder geradezu bösartiger Apps in diese Stores. Im Dezember 2017 wurden beispielsweise Hunderte gefälschte Kryptowährungs-Apps im Apple App Store und bei Google Play veröffentlicht. Diese Apps haben Benutzer dazu verleitet, Benutzernamen und Passwörter an echte Kryptowährungs-Handelsseiten weiterzugeben, und die bösartigen Akteure hinter diesen gefälschten Apps konnten virtuelle Währungen stehlen. Im November 2017 war die drittbeliebteste App in der Kategorie „Finanz-Apps" des Apple App Store, MyEtherWallet, eine Fälschung.




*MyEtherWallet war eine gefälschte App, die Ende 2017 zeitweise die dritthäufigste heruntergeladene App im Apple App Store war.*

**App Stores von Drittanbietern:** Benutzer können absichtlich oder versehentlich auf inoffizielle App-Stores auf Android- und iPhone-Geräten zugreifen. Diese App-Stores nutzen häufig ein Konfigurationsprofil, das auf einem Gerät durch den Besuch einer Webseite installiert wird. Sobald ein solches Profil auf dem mobilen Gerät installiert ist, kann der Benutzer auf App-Stores von Drittanbietern zugreifen und Apps auf das Gerät herunterladen. Diese Apps werden keiner Verifizierung oder Sicherheitsprüfung unterzogen und können verwendet werden, um Phishing-URLs, schädliche Inhalte und sogar schädliche Apps auf dem Gerät des Benutzer zu installieren.

# DIE FINANZIELLE MOTIVATION DER MOBILE DEVICE-PHISHER

Die Hauptmotivation für Mobile Device-Phisher ist finanzieller Natur. Phisher, die Benutzer von mobilen Geräten angreifen, können ihre Angriffe auf folgende Weise zu Geld machen:

**Online-Anmeldeinformationen stehlen und verkaufen:** Es gibt geschäftige Online-Märkte für den Verkauf und Kauf gestohlener Online-Zugangsdaten. Phisher verdienen duech ihre Angriffe Geld, indem sie Benutzernamen und Passwörter auf diesen Märkten verkaufen.

**Zugriff auf Unternehmenssysteme erhalten:** Durch den Erwerb von Anmeldeinformationen für Unternehmenssysteme mittels Phishing, können Benutzer von mobilen Geräten, die sowohl für Unternehmen als auch für den persönlichen Gebrauch verwendet werden, Angreifern Zugriff IT-Systeme des Unternehmens gewähren. Dieser Zugriff durch Phishing von Benutzernamen und -Kennwörter, VPN-Anmeldeinformationen und sogar Handy-PINs erhalten werden. PINs von Mobilfunkanbietern sind hilfreich, wenn der Angreifer die Telefonnummer des Opfers auf sein eigenes Gerät übertragen möchte und anschließend dessen SMS-Nachrichten und Anrufe erhält. Normalerweise geschieht dies, um zweistufige Authentifizierungssysteme (2FA) von Unternehmen zu umgehen, die zusätzlich zu Benutzernamen und Kennwörtern SMS-Kurzmitteilungscodes verwenden. Sobald der Zugriff auf interne IT-Systeme erreicht ist, können Angreifer diesen Zugriff entweder an Datendiebe und Spione verkaufen oder sie verwenden, um in Unternehmenssysteme einzudringen und Kundendaten zu stehlen.

**Zugang zu Bank- und Zahlungsdiensten erhalten:** Phisher verwenden häufig gestohlene Anmeldeinformationen, die von Phishing-Angriffen auf mobilen Geräten abgerufen wurden, um Zugang zu Bank- und Zahlungsdiensten zu erhalten. Dies ist eine Variante des mittlerweile üblichen E-Mail-Phishing-Angriffs, um Zugriff auf Online-Konten zu erhalten.

**Kryptowährung stehlen:** Eine neue Form des Phishing-Angriffs auf mobilen Geräten konzentriert sich darauf, Zugriff auf Kryptowährungen zu erhalten, die auf dem mobilen Gerät oder in einer Online-Börse gespeichert werden können. Angreifer sind sehr begierig darauf, diese Daten zu stehlen, da sie auf diese Weise sehr leicht auf Kryptowährungsfonds zugreifen und sie an Adressen verlegen können, an denen Opfer ihre Vermögenswerte nicht wiederherstellen können. Dieser gezielte Diebstahl von Berechtigungsnachweisen hat in den letzten drei Jahren für das App-, E-Mail- und SMS-Phishing dieser Ziele enorm zugenommen. Neben dem Diebstahl der Anmeldeinformationen einzelner Benutzer wird Phishing von mobilen Geräten häufig verwendet, um sich an Führungskräfte in diesen Unternehmen zu wenden, um Zugriff auf größere Reserven von Kryptowährungen zu erhalten.

# LÖSUNGEN FÜR DIE SICHERUNG VON MOBILGERÄTEN UND BENUTZERN GEGEN PHISHING

Die APWG empfiehlt einen mehrschichtigen Ansatz, um mobile Geräte vor Phishing-Angriffen zu schützen. Ohne alle vier Schichten sind mobile Geräte und ihre Benutzer in vielen verschiedenen Zustellungskanälen, einschließlich E-Mail, SMS/Text/iMessage und Apps, anfällig. Wenn beispielsweise Geräte nicht gesperrt sind und strikt auf die Verwendung für Unternehmensfunktionen beschränkt sind, d. h. sie können nur auf Unternehmensanwendungen zugreifen und nicht für Textnachrichten verwendet werden, können sie nicht durch einen auf Server beschränkten E-Mail-Filteransatz geschützt werden. Obwohl dies insgesamt unrealistisch ist, ist es die sicherste Lösung. Die starke Verschiebung auf BYOD für mobile Geräte erweitert die Bedrohungslandschaft für Phishing dramatisch, was den Bedarf an umfassenderen Schutzfunktionen verstärkt. Dieser vierstufige Ansatz zum Schutz von mobilen Unternehmensgeräten gegen Phishing- und Spear-Phishing-Angriffe umfasst folgende bewährten Methoden:

## 1 Serverbasierter Phishing-Schutz

Die erste Verteidigungslinie gegen Phishing auf mobilen Geräten besteht in einem robusten, serverbasierten Phishing-Schutz. Dieser Schutz muss aus Spam-Filtern, Phishing-Erkennung, BEC-Phishing-Erkennung und Spear-Phishing-Erkennung bestehen. Für den Schutz mobiler Geräte ist dies aber nicht unbedingt ausreichend.

## 2 Gerätebasierter URL-Schutz

Die zweite Verteidigungslinie gegen Phishing auf mobilen Geräten ist ein gerätebasierter URL-Filter für E-Mail, SMS/Text/iMessage und App-Phishing. Da mobile Geräte sowohl für geschäftliche als auch für private Zwecke verwendet werden, und zahlreiche Möglichkeiten bestehen, Inhalte und Nachrichten zu empfangen, ist es unbedingt erforderlich, dass Geräte über einen integrierten URL-Schutz verfügen. Die große Mehrheit der Phishing-Angriffe weist ein Opfer auf eine URL mit überzeugenden Inhalten hin, die den Benutzer dazu verleitet, Anmeldeinformationen (Benutzername, Kennwort, VPN-Kennwort, PIN) preiszugeben oder gefährliche Apps und Konfigurationsprofile zu installieren. URL-Schutz, der sich nicht nur auf das E-Mail-Konto eines Unternehmens beschränkt, sondern auch persönliche E-Mail-Konten, SMS/Text/iMessage und den Inhalt von heruntergeladenen Apps umfasst, ist von entscheidender Bedeutung.

## 3 Gerätebasiertes Sicherheits-Profiling

Unternehmen sollten gerätebasierte Sicherheitsprofile bereitstellen, um zu ermitteln, ob Geräte absichtlich oder versehentlich durch gezieltes Phishing oder Einwirkung durch bösartige Apps oder gefälschten Netzwerkverkehr anfällig gemacht wurden. Diese Profile sollten Betriebssystemversionen und Patch-Level, installierte Konfigurationsprofile und Zertifikate überprüfen und nach schädlichen Apps suchen.

## 4 Aufklärung des Benutzers

Phishing- und Spearfishing-Angriffe haben eines gemeinsam: Sie erfordern einen unwissenden oder unzureichend ausgebildeten Menschen auf der Empfängerseite. Das Problem für Sicherheitsteams liegt in der zunehmenden Komplexität heutiger Angriffe. Die Kontaktaufnahme durch Social Engineering und Social Hacking erscheint oft authentisch, enthält glaubwürdige persönliche Informationen und scheint von einer legitimen Adresse zu stammen.

**Die starke Verschiebung auf BYOD für mobile Geräte erweitert die Bedrohungslandschaft für Phishing dramatisch, was den Bedarf an umfassenderen Schutzfunktionen verstärkt.**

# BRINGEN SIE IHREN MITARBEITERN BEI,

## GEFÄLSCHTE E-MAILS ZU ERKENNEN

In der Vergangenheit enthielten Phishing-E-Mails häufig schlechte Grammatik, Tippfehler oder täuschten besondere Dringlichkeit vor oder wiesen andere verräterische Anzeichen für gefälschte Korrespondenz auf. Aufgrund der enormen Fortschritte bei Phishing- und Spear-Phishing-Angriffen in der jüngeren Vergangenheit, ist die einzige zuverlässige Verteidigung jedoch Folgende:

- Öffnen Sie keine Anlagen, die nicht bekannt oder angefordert sind.
- Antworten Sie nicht auf unbekannte E-Mails.
- Geben Sie keine persönlichen Informationen wie Kredit- oder Debitkartennummern, Bankkontoinformationen, Führerscheinnummern, Passwörter oder Ihren vollständigen Namen preis. Legitime Unternehmen werden diese Dinge niemals in E-Mails, Texten oder ausgehenden Telefonaten anfordern.
- Seien Sie vorsichtig, wenn Sie eine unerwartete Zahlungsbenachrichtigung per E-Mail erhalten.
- Seien Sie vorsichtig bei unbekannten Anfragen von Mitgliedern auf Facebook, LinkedIn usw. Wenn Sie beispielsweise eine Anfrage von einem LinkedIn Mitglied erhalten, sollte die Anmeldung bei Ihrem LinkedIn Konto dieselbe Anfrage zeigen. Wenn nicht, haben Sie einen „Phish" erwischt.

## WIE MAN GEFÄLSCHTE WEBSITES ERKENNT

Ein Phisher fordert Sie oft dazu auf, auf einen Link zu klicken, der Sie zu einer Website führt, die rechtmäßig aussieht. Doch gerade das Anklickeneines solchen Links könnte Sie zu einer Seite weiterleiten, die möglicherweise Malware auf Ihren Computer herunterlädt. Wenn Sie auf der Seite nach Ihrem Kennwort, Kredit- oder Bankdaten und / oder SSN gefragt werden, schließen Sie Ihren Browser. Dies sind Anzeichen einer gefälschten Website:

- In der Verganganheit galt es als bewährte Vorgehensweise, die URL auf unsichere Links zu überprüfen. Sichere URLs beginnen mit https. Anspruchsvolle Phisher verwenden jedoch immer häufiger sichere Verbindungen.
- Wenn Sie auf eine URL klicken und diese zu einer völlig anderen Website weiterleitet, schließen Sie Ihren Browser.

## WIE SIE VERMEIDEN KÖNNEN, SMISHING-OPFER ZU WERDEN

Seien Sie vorsichtig bei Textnachrichten, die eine dringende Aufforderung zum Anrufeneiner gefälschten Telefonnummer oder zum Besuchen einer URL bezüglich derAbrechnung oder eines anderen Problems enthalten. Daraufhin wird versucht, persönliche private Informationen zu erlangen.

## WIE SIE VERMEIDEN KÖNNEN, VISHING-OPFER ZU WERDEN

Bei diesem Sprachtelefonie-Äquivalent zum Phishing verwendet ein Betrüger ein automatisiertes System, um Sprachanrufe zu tätigen. Normalerweise erwähnen die Anrufer ein „dringendes Kontoproblem" und bitten Sie, Kontoinformationen mitzuteilen, um Abhilfe zu schaffen. Ein Beispiel für einen erfolgreichen Versuch ist:

> *„Hier ist (XYZ). Um das Aussetzen Ihrer mobilen Dienste zu vermeiden,*
> *geben Sie bitte Ihre PIN ein, um diese dringende Nachricht der Buchhaltung zu hören."*

Antworten Sie auf keine Informationsanforderung in diesen Aufrufen.

# ÜBER DIE ANTI-PHISHING WORKING GROUP

Die APWG (Anti-Phishing-Working Group) wurde 2003 gegründet. APWG ist eine globale Industrie-, Strafverfolgungs- und Regierungskoalition, die sich darauf konzentriert, die globale Reaktion auf elektronische Kriminalität zu vereinheitlichen. Die Mitgliedschaft steht qualifizierten Finanzinstituten, Online-Händlern, ISPs und Telekommunikationsunternehmen, der Strafverfolgungsbehörden, Lösungsanbietern, multilateralen Vertragsorganisationen, Forschungszentren, Handelsverbänden und Regierungsbehörden offen. An der APWG sind weltweit mehr als 2.200 Unternehmen, Regierungsbehörden und NGOs beteiligt.

Die Websites www.apwg.org> und <education.apwg.org> von APWG bieten der Öffentlichkeit, Industrie und Regierungsbehörden praktische Informationen über Phishing und elektronisch vermittelten Betrug sowie Hinweise auf pragmatische, technische Lösungen, die sofortigen Schutz bieten. Die APWG ist Mitgründer und Co-Manager der Stop. Think. Connect. Messaging Convention, die globale Online-Sicherheits-Gemeinschaft der Öffentlichkeit <https://education.apwg.org/safety-messaging-convention/> und Gründer/Kurator des eCrime Researchers Summit, die weltweit einzigen von Experten begutachtete Konferenz, die sich speziell mit Studien zur elektronischen Kriminalität befasst.

APWG berät hemisphärische und globale Handelsgruppen und multilaterale Vertragsorganisationen wie die Europäische Kommission, die Untergruppe für Hochtechnologiekriminalität der G8, das Übereinkommen des Europarates gegen Cyberkriminalität, das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung, die Organisation für Sicherheit und Zusammenarbeit in Europa, Europol EC3 und die Organisation der amerikanischen Staaten.

APWG ist Mitglied der Steuerungsgruppe der Commonwealth Cybercrime-Initiative im Commonwealth of Nations.

Für weitere Informationen besuchen Sie die Website der Anti-Phishing Working Group auf www.antiphishing.org, www.apwg.org und www.apwg.eu.