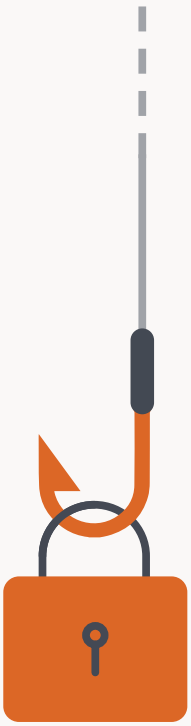
Phishing-Trends Bericht 2021

2021 hat Phishing jede Art der Kommunikation infiltriert, von E-Mail bei der Arbeit und im persönlichen Bereich zu SMS, Sozialen Medien und sogar Werbung.

Social-Engineering-Angriffe, die einst auf die E-Mails von Unternehmen beschränkt waren, stellen heutzutage die gefährlichste Bedrohung für Cybersicherheit dar, die Organisationen auf allen Plattformen zu bekämpfen haben – einschließlich Desktops und Mobilgeräten.

Warum? Weil es für Angreifer einfacher ist, eine Person zu betrügen und Daten über einen Phishing-Angriff zu erbeuten, als das robuste Betriebssystem eines Geräts zu täuschen. Im Zeitalter Cloud-orientierter Unternehmen sind die Anmeldedaten von Anwendern sogar viel wertvoller, da sie Zugriff auf vertrauliche Daten gewähren, die außerhalb des Geräts in SaaS-Anwendungen, Online-Datenspeichern und Rechenzentren gespeichert und verwaltet werden.

Die Durchführung von Phishing-Angriffen hat sich weit über schlecht formulierte E-Mails hinaus entwickelt, die „nicht beanspruchte Lotteriegewinne“ anbieten. Diese Attacken sind nicht nur mehr persönlich abgestimmt und überzeugender, sie erreichen auch Benutzer an mehr Orten als je zuvor, und gehen zunehmend über die Verbraucher hinaus, um Passwörter und Daten von Unternehmen zu erbeuten. Das geht vor allem auf die zunehmende Akzeptanz von Mobilgeräten zurück.



Phishing-Angriffe täuschen eine zunehmende Anzahl von Mobilgerät-Benutzern

Ein Großteil des Web-Datenverkehs ist jetzt mit Benutzern von Mobilgeräten assoziiert. Daher ist es nicht überraschend, dass Hacker dies ausnutzen, indem sie Attacken spezifisch auf Mobilplattformen zuschneiden. Mobilgeräte haben kleinere Bildschirme und nutzen eine Reihe von visuellen Kurzbefehlen, was bedeutet, dass es viel schwieriger als auf dem Desktop ist, verdächtige URLs oder schädliche Absender zu erkennen. Benutzer werden auf Mobilgeräten auch aufgrund ihrer portablen Natur und dem Gefühl eines persönlichen Geräts mehr abgelenkt und sind dadurch anfällig.

Angreifer produzieren weiterhin immer überzeugendere Phishing-Websites, die auf Benutzer von Mobilgeräten ausgerichtet sind, da bis zu 1 von 10 Mobilgeräte-Benutzern auf Phishing-Angriffe hereinfallen. Das bedeutet nicht, dass man nur Nachrichten empfängt, sondern tatsächlich auf sie klickt.

Unten stehende Grafik zeigt einen Zuwachs von 160 % bei der Zahl der Mobilgerät-Benutzer, die in den vergangenen 12 Monaten Opfer von Phishing-Angriffen wurden. Das hat nichts mit dem Volumen der Online-Angriffe zu tun, sondern zeigt die Zahl der Personen, die darauf hereinfallen. Dieser Anstieg der Zahl von Menschen, die den Köder schlucken, geht wahrscheinlich auf verbesserte Methoden der Angreifer zurück. Sie nutzen jetzt vertrauenswürdig Apps zur Übermittlung der Nachrichten, sie registrieren überzeugende Domains und imitieren bekannte Marken, um mehr Benutzer mit weniger Aufwand zu erreichen.

1 von 10

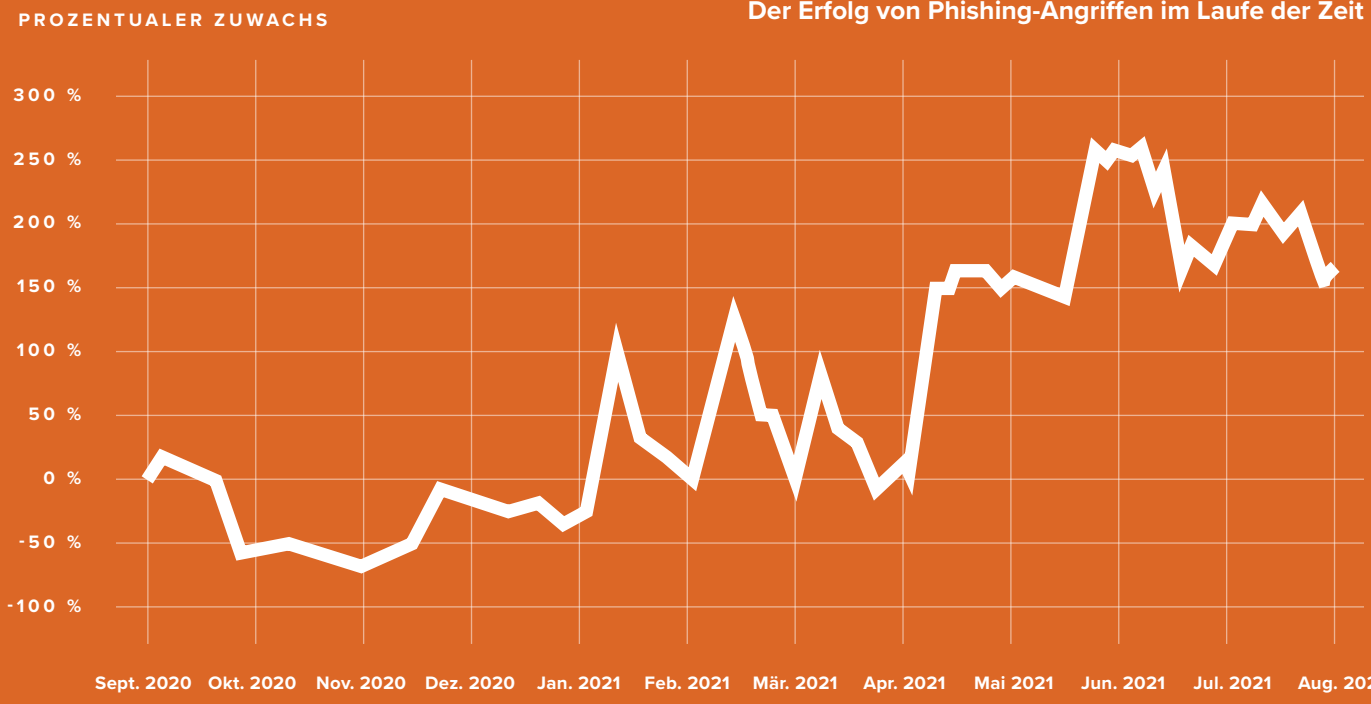
Personen klicken auf Phishing-Links, während sie ihre Mobilgeräte benutzen

Quelle: Wandera, eine Tochterfirma von Jamf

Die Anzahl der Mobilgeräte-Benutzer, die auf Phishing-Angriffe hereinfallen, hat sich gegenüber dem Vorjahr um 160 % erhöht

Quelle: Wandera, eine Tochterfirma von Jamf

Der Erfolg von Phishing-Angriffen im Laufe der Zeit



Quelle: Wandera, eine Tochterfirma von Jamf

Phishing-Angriffe sind auf Mobilgeräten schwieriger zu erkennen

Die heute für die Telarbeit eingesetzten sehr portablen Geräte erschweren es, Phishing-Angriffe zu erkennen.

- Eine zunehmende Verwendung von Mobilgeräten führt zu kleineren Bildschirmgrößen, was weniger Platz bietet, um die Legitimität einer Website zu beurteilen.
- Verbesserungen bei der Benutzeroberfläche haben zu Designentscheidungen geführt, die normalerweise die bereits kleine Adressleiste verbergen, während der Benutzer nach unten scrollt, um Platz für Seiteninhalte zu schaffen.
- Abgelenkte Benutzer, die mehrere Geräte einsetzen und mit einer Vielzahl von Apps kommunizieren und zusammenarbeiten, neigen dazu, rasch durch die verschiedenen Seiten und Benachrichtigungen zu gehen. Darüber hinaus markieren viele Entwickler die Schaltfläche „Akzeptieren“ oder „OK“ in Aufforderungen, sodass Benutzer diese oft automatisch annehmen, ohne sie genauer anzusehen.
- Optimierte visuelle Gestaltung, die Inhalten statt Metadaten mehr Platz auf dem Bildschirm bietet, hindert Benutzer daran, das Verlinkungsziel vor dem Klicken zu sehen oder zu bewerten.
- Kurz-URL-Dienste wie Bitly oder Owly – häufig in Textnachrichten verwendet wird – verbergen die vollständige Domain.

Phishing wird außerhalb von E-Mail geliefert, wo Leute das nicht erwarten.

Üblicherweise haben Sicherheitsmaßnahmen das Phishing als E-Mail-Problem von Unternehmen betrachtet. Dabei wird die Lösung ins E-Mail-Programm integriert, statt ins Gerät. In dem Maße, wie Leute zunehmend mobil arbeiten, verwenden sie (1) mehr Apps, die nicht geschützt sind, und (2) befinden sich außerhalb des Perimeters und profitieren daher nicht von den Schutzmaßnahmen im Firmengelände.

Die Geräte für Endnutzer bieten zunehmend eine konsolidierte Kommunikationsplattform, bei der sie zahlreiche Messaging- und Social-Media-Apps mit direkter Benachrichtigung in der App haben. MacBooks mit Apple Chip können nicht nur macOS Apps ausführen, sondern auch iOS Apps und Windows usw., um eine kohärente Computererfahrung zu bieten. Messaging-Apps werden bei den Abwehrmaßnahmen der Organisation oft übersehen, und bieten daher Angreifern ein Einfallstor.

Die Konzentration auf Mobilgeräte hat es Hackern erlaubt, vom vertrauenswürdigen Bereich der E-Mail auf eine Vielzahl neuer Verteilungsmethoden wie SMS, WhatsApp, Messenger, Instagram und LinkedIn überzugehen – Dienste, denen Benutzer vertrauen.





Das Vorhängeschloss wird verwendet, um Benutzer weiter zu täuschen.

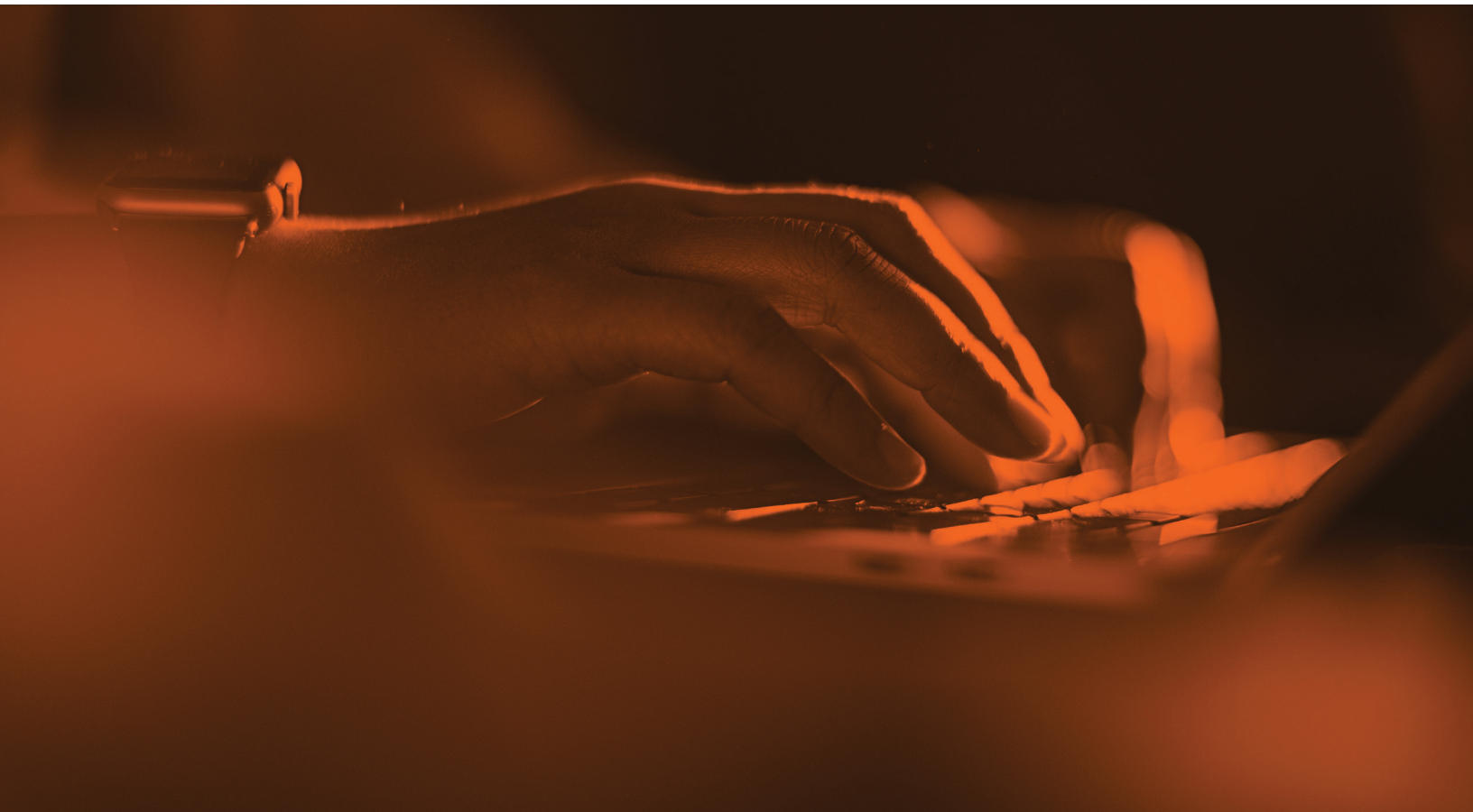
Früher war es einfach, die Adressleiste auf ein Vorhängeschloss zu überprüfen um so schädliche Domains zu entdecken. Aber jetzt gibt es zahlreiche kostenlose Dienste online, die Angreifer nutzen können, um schnell und mühelos eine SSL-Zertifizierung für bösartige Phishing-Websites zu erhalten. Leider ist das effektiv, weil Benutzer glauben, dass das Vorhängeschloss-Symbol vor einer URL ein verlässlicher Hinweis darauf ist, dass eine Website sicher ist. Da die Kostenbarriere verschwunden ist, haben Angreifer jeden Grund dafür, ihre bösartigen Websites zu verschlüsseln.

93 % der der Phishing-Domains werden auf einer „sicheren“ Website gehostet, die in der URL-Leiste ein Vorhängeschloss anzeigt

Quelle: Wandera, eine Tochterfirma von Jamf

Heutzutage nutzen 93 % der erfolgreichen Phishing-Websites HTTPS-Verifizierung, um ihre bösartige Natur zu verbergen. Unseren Daten zufolge ist diese Zahl dramatisch über den Wert von 65 % im Jahr 2018 angestiegen.

Quelle: Wandera, eine Tochterfirma von Jamf



Punycode macht es schwerer, böswillige Domains zu identifizieren

Angreifer verwenden zunehmend Punycode, um es zu erschweren, ihre Phishing-Domains zu erkennen. Punycode verwandelt Wörter mit Unicode-Zeichen (beispielsweise in Alphabeten wie Kyrillisch, Griechisch und Hebräisch) in ASCII-Zeichen, die Computer verstehen können.

Die Ursprünge von Punycode-Angriffen gehen auf eine Zeit zurück, als Browser nicht Unicode unterstützten und nur ASCII zur Anzeige von URLs verwendeten. Damals nutzten Angreifer diese Zeichensätze, da sie Domains registrieren konnten, die existierenden und vertrauenswürdigen Domains ähnelten. Dadurch wurde der Browser missbraucht, um Benutzer zu täuschen, dass sie mit einer Website kommunizierten, wenn sie tatsächlich mit einer anderen Website kommunizierten. Unicode-Zeichen erzeugen Domainnamen, die dem nackten Auge vertraut vorkommen, aber in Wirklichkeit auf einen anderen Server Server verweisen oder eine nicht vertraute Domain verlinken.

Unseren Daten zufolge verwendeten in den vergangenen 12 Monaten 2 % der erfolgreichen Zero-Day-Phishingangriffe Punycode. Nachfolgend einige Beispiele. Können Sie die Unicode-Zeichen in den folgenden Domains erkennen?

2 % der Phishing-Angriffe, denen Benutzer zum Opfer fielen, enthielten Punycode

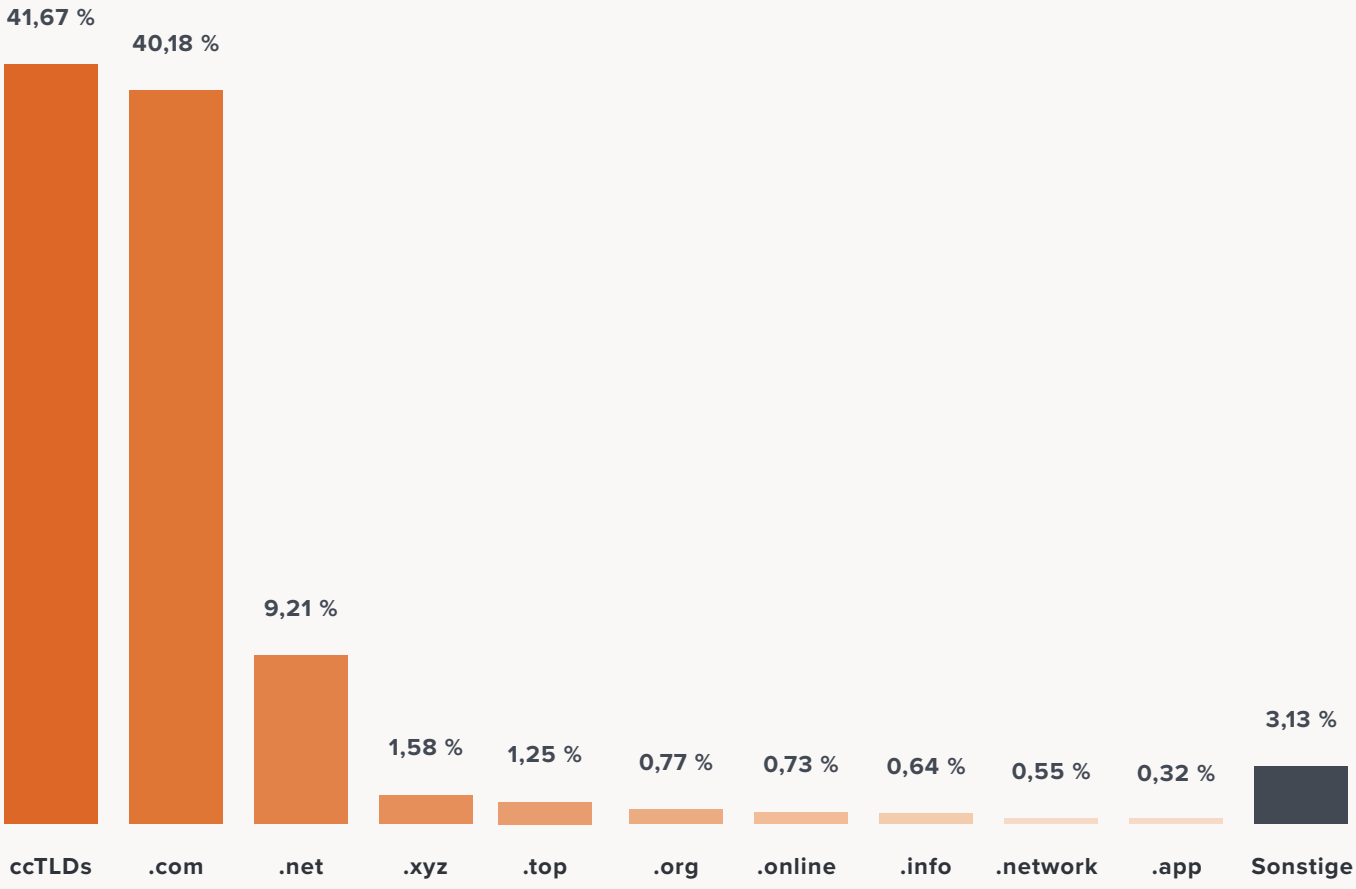
Quelle: Wandera, eine Tochterfirma von Jamf

MARKE	WAS DER BENUTZER SIEHT (UNICODE)	DER „ENTSCHLÜSSELTE“ PUNYCODE
Google	https://googĺe.com	xn--googe-95a.com
Starbucks	https://starbucks.com	xn--starucks-hpd.com
Rolex	https://rolẹx.com	xn--rolx-nu5a.com
Paypal	https://t.paypal.com	t.xn--ayal-9ndc.com
Facebook	https://www.facebook.com⁄login.en.do	www.facebook.xn--comlogin-g03d.en.do

Obskure Top-Level-Domains machen alles schlimmer.

Top-Level-Domains (TLD) waren früher nur .com, .net, .org usw. In den letzten Jahren verwenden mehr Domains unterschiedliche Ländercode Top-Level-Domains (ccTLD) und unternehmensspezifische TLDs (wie .attorney, .technology, .airline) sind ebenfalls aufgetaucht. Nachfolgend der Anteil der Top-Level-Domains, die wir bei erfolgreichen Phishing-Angriffen gesehen haben. Die Gefahr ist dabei, dass Benutzer einen Markennamen sehen, den sie erkennen, aber mit einem ungewöhnlichen TLD. Beispielsweise kann ein Hacker microsoft.xyz registrieren, um einen Phishing-Angriff in Verbindung mit Microsoft zu hosten. Wenn das entdeckt wird, wird es durch microsoft.info oder microsoft.network usw. ersetzt.

Nachfolgend der Anteil der TLDs bei erfolgreichen Phishing-Angriffen, die in den vergangenen 12 Monaten auf unserer Plattform erkannt wurden. Die üblichen .com und .net TLDs sind am populärsten, neben einer Reihe von ccTLDs wie .ru, .uk und .co.



Quelle: Wandera, eine Tochterfirma von Jamf

Hauptpunkt: Wenn Sie das Vorhängeschloss, Punycode und ungewöhnliche TLDs zusammen verwenden, ist es sehr leicht, ein überzeugendes Phishing-Domain zu erstellen, dass selbst die größten Marken imitiert.

Die 10 häufigsten Marken in erfolgreichen Phishing-Angriffen

Um die Erfolgsrate eines Angriffs zu erhöhen, müssen schädliche Akteure gut auswählen, welches Unternehmen sie nachahmen wollen.

Angreifer wechseln von regionalen Attacken (in denen z. B. die Marke einer örtlichen Bank verwendet wird) zu solchen, die globale, technologieorientierte Marken einbeziehen. Leute werden eher einem Phishing-Angriff zum Opfer fallen, wenn der Köder für eine Website ist, auf der sie tatsächlich einen Account haben. Da die Single-Sign-On Technologie in mehr und mehr Apps integriert wird, bieten Anmeldedaten für große einflussreiche Unternehmen wie Apple, Google, Amazon und Microsoft Zugriff auf mehr als nur E-Mail. Sie sind der Universalschlüssel und öffnen neue Schichten von persönlichen und geschäftlichen Daten. Dabei sind nicht diese Unternehmen schuld, sondern werden lediglich von bösartigen Akteuren benutzt, da jeder sie kennt und sie reiche Quellen wertvoller Informationen bieten.

Schädliche Akteure zielen zunehmend auf Apps, die für die Arbeit verwendet werden, wie Office 365 und die G-Suite von Google. Da Unternehmen sich zunehmend bemühen, ihre Unternehmens-Assets in die Cloud zu verschieben, ist das ein großes Problem. Ein Fehler eines Mitarbeiters, der Ziel eines cleveren Phishing-Angriffs wird (indem er beispielsweise die Anmeldedaten für Google Drive bestätigen soll) kann einem Hacker Zugriff zu Unternehmensdaten in diesen beliebten Cloud-Anwendungen bieten.

Unseren Untersuchungen zufolge sind die drei führenden Marken in Phishing-Angriffen, mit denen Benutzer 2021 dazu gebracht wurden, auf Phishing-Links zu klicken, Apple, PayPal und Amazon, die für 43 %, 27 % und 9 % der jeweiligen Angriffe verwendet wurden.

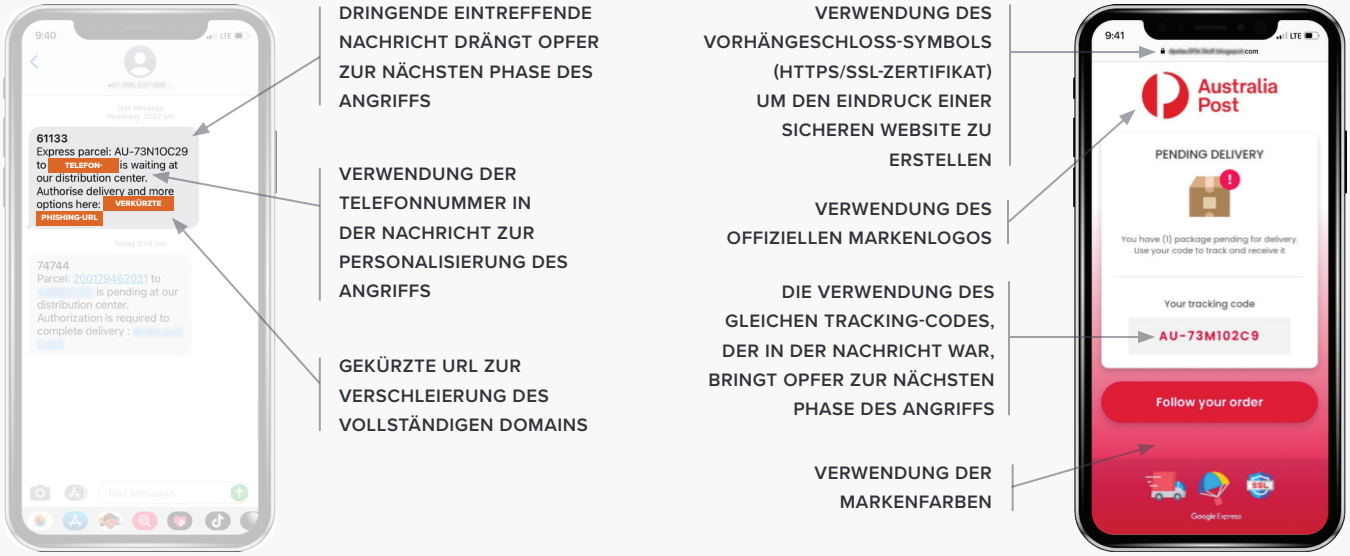
Die 10 häufigsten Marken in Phishing-Kampagnen im Jahr 2021

1. **Apple**
2. **PayPal**
3. **Amazon**
4. **Chase**
5. **Facebook**
6. **Google**
7. **Twitter**
8. **Netflix**
9. **Microsoft**
10. **Wells Fargo**

Quelle: Wandera, eine Tochterfirma von Jamf

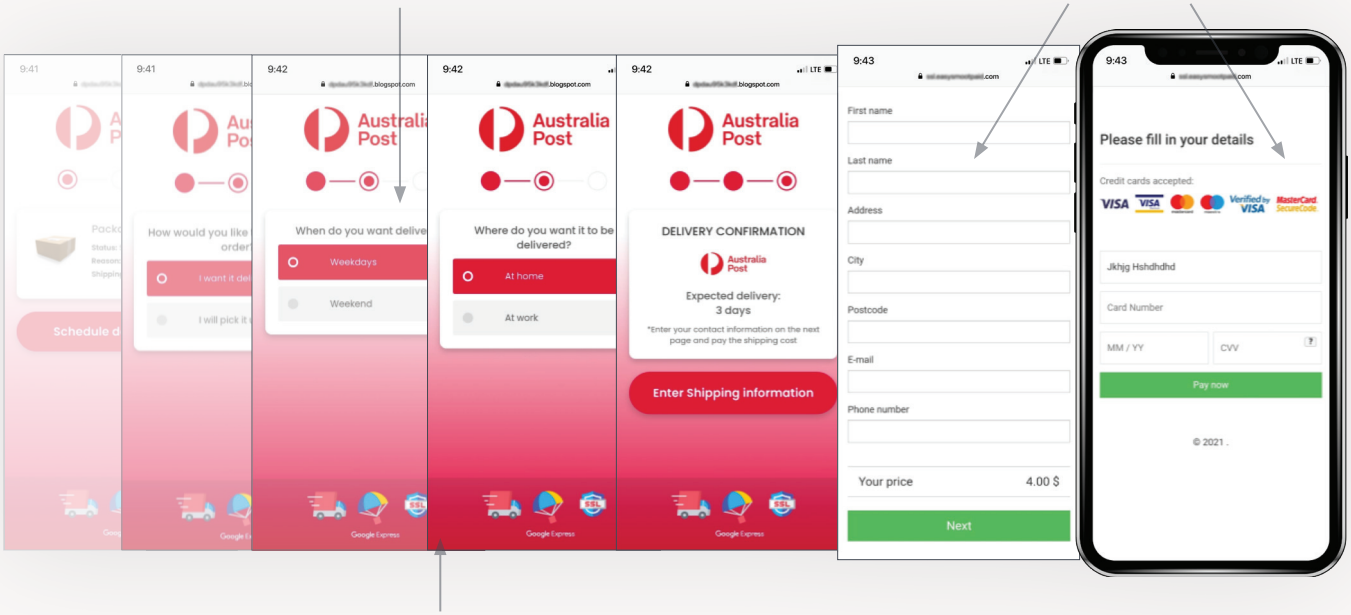
Phishing-Kampagnen-Spotlight – Australia Post

Unsere Forscher untersuchten eine Phishing-Kampagne, in der mehrere verdächtige Textnachrichten gemeldet wurden. Die Nachrichten hatten etwas mit der Lieferung von Paketen zu tun und verwendeten die bekannte Marke Australia Post (Australia Post ist das Äquivalent der Deutschen Post, daher wären alle, die in Australien leben und Post empfangen, potenzielle Opfer). Das ist ein opportunistischer Angriff, da sich viele Menschen in Australien während der strengen und wiederholten COVID-19 Lockdowns auf die Lieferung nach zuhause verließen. Wie andere große Marken, die in Phishing-Angriffen verwendet werden, hat Australia Post nichts falsch gemacht – die Marke wird von den Angreifern einfach wegen ihres Bekanntheitsgrads verwendet.



INTERAKTIVE WEBSITE MIT KONSISTENTEN SYMBOLEN, SCHRIFTARTEN, MARKENFARBEN USW.

EINGABE PERSÖNLICHER DETAILS WIE ANMELDEDATEN, FINANZIELLE DATEN UND ANDERE PERSONENBEZOGENE INFORMATIONEN



WEITERENTWICKLUNG ZUM SOCIAL-ENGINEERING-EXPLOIT

Quelle: Wandera, eine Tochterfirma von Jamf

Es gibt viele schlecht aufgebaute Phishing-Kampagnen da draußen. Manchmal stimmt die Nachricht nicht einmal mit den Seiteninhalten überein, oder der Seiteninhalt ist ein sehr genereller Betrug. Der Australia Post Phishing-Angriff ist etwas komplexer, da es eine Kontinuität zwischen der Nachricht und den Seiteninhalten gibt, um das Opfer zu überzeugen, eine Paketauslieferung zu autorisieren.

Obwohl das ein gut ausgeführter Angriff ist, gibt es einige offensichtliche Anzeichen eines Phishings. Erstens verwendet die URL nicht das Domain auspost. Zweitens ist das Branding überzeugend, aber es stimmt nicht perfekt mit der legitimen Website von Australia Post überein. Drittens wird der Benutzer zu einer anderen Domain außerhalb der Marke umgeleitet, die eine Zahlung erfordert, obwohl dies für die Autorisierung einer Lieferung normalerweise nicht erforderlich ist. Und letztlich verwenden die Australier die Schreibung „centre“ und nicht „center“ – wenn man also aufpasst, kann man Phishing-Attacken selbst an winzigen Details erkennen!

Nicht vergessen:

Wenn Sie in diesen Situationen eine überzeugend klingende Nachricht erhalten, empfehlen wir Ihnen, direkt zur App oder Website Ihres Dienstes zu gehen, statt etwas in der E-Mail oder Nachricht anzuklicken.

Eine schnelle Prüfung

Viele Phishing-Websites werden nur für einige Stunden online veröffentlicht, bevor Hacker zu einem völlig neuen Hosting-Server wechseln. Das ermöglicht es ihnen, unentdeckt zu bleiben und Kampagnen fortzusetzen, ohne blockiert zu werden. Das Risiko für Benutzer ist in diesen ersten kritischen Stunden am höchsten, bevor die statische, listenbasierte Threat Intelligence aktualisiert wird.

Wenn bei dem oben erwähnten Australia Post Angriff die Phishing-Domain gemeldet und gesperrt wird, muss der Angreifer lediglich eine neue Domain registrieren und den Angriff erneut starten, bis auch diese neue Domain gemeldet wird, und so weiter. Wenn man die Anzahl der Top-Level-Domains bedenkt, die es gibt, und die zahlreichen Subdomains in legitimen URLs (wie login., mobile. oder en.), versteht man, wie ein Angreifer eine derartige Kampagne fortführen kann. Kombinieren sie Ihre eigene Phishing-URL aus einigen Beispielen weiter unten und fragen Sie sich dann, ob Sie darauf hereinfallen würden?

SUBDOMAIN	MARKE	TOP-LEVEL-DOMAIN
tracking.	aus-post	.com
feedback.	auspost	.net
mobile.	australiapost	.review

Empfehlungen

Phishing-Angriffe nutzen den anfälligsten Teil einer Organisation – die Mitarbeiter. Mitarbeiter sind oft das wertvollste Asset eines Unternehmens, aber wenn es um die Datensicherheit geht, sind sie oft auch die größte Schwachstelle.

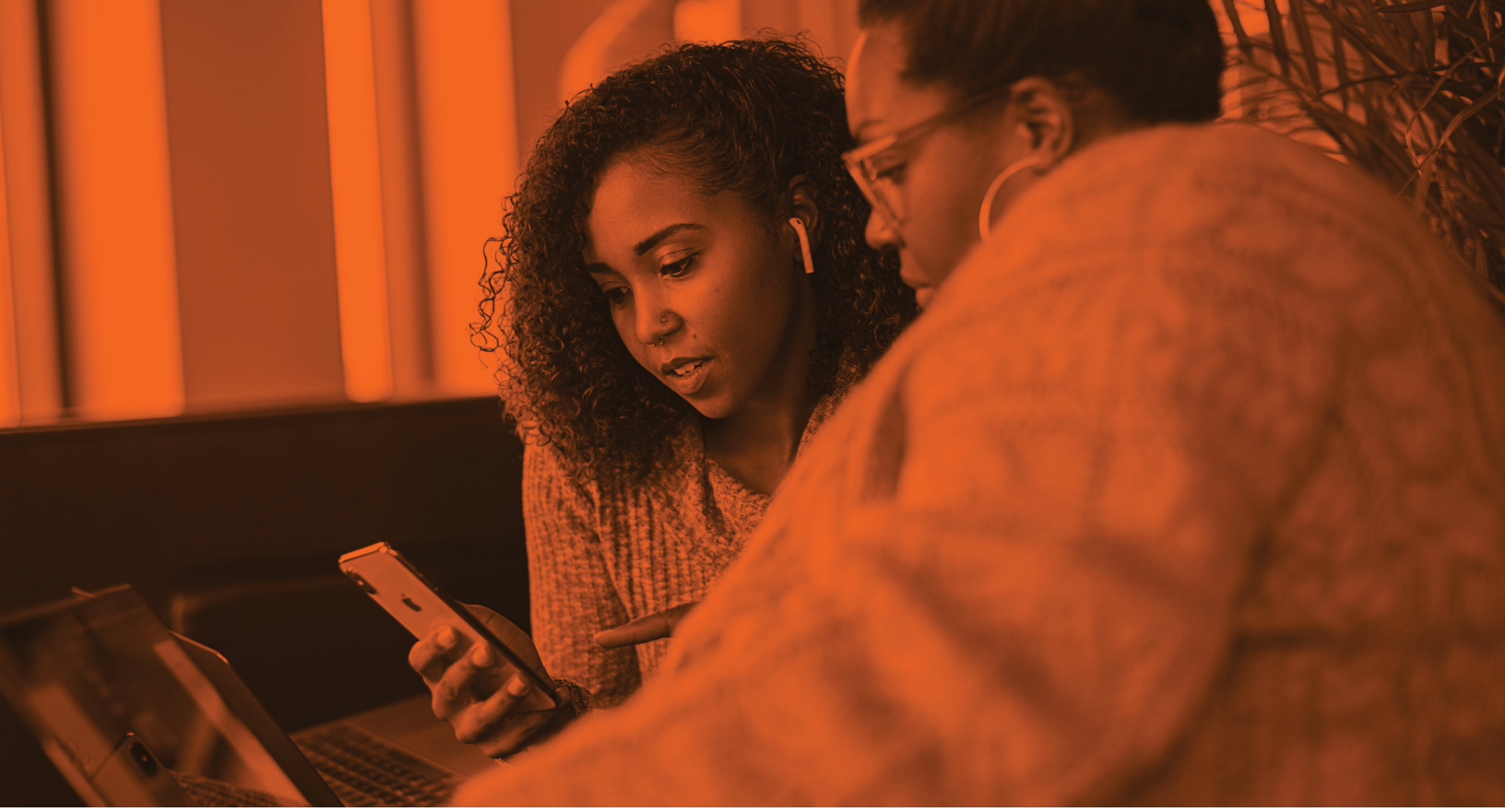
Deshalb ist eine Zero-Day Phishing-Lösung – besonders eine Lösung, die über alle Kommunikations-Apps hinweg funktioniert, nicht nur für E-Mail – entscheidend, um sowohl die üblichen Attacken zu stoppen, als auch die anspruchsvolleren Angriffe, die auf Ihr Unternehmen abzielen.

Sie waren das Opfer eines Phishing-Angriffs. Was nun?

- Ändern Sie alle Ihre Passwörter für die kompromittierten Accounts, sowie Accounts, welche die gleichen oder ähnliche Passwörter verwenden, wie die vom Hacker erbeuteten.
- Wenn Sie Ihre Kreditkartendaten auf der Phishing-Seite eingegeben haben, lassen Sie Ihre Karte sperren.
- Nehmen Sie Ihren Computer offline oder löschen Sie Ihren E-Mail-Account, damit Sie keine Phishing-Links an Ihre Kontaktlisten senden.
- Wenden Sie sich an das Unternehmen oder die Person, die bei diesem Angriff nachgeahmt wurde – das könnte Ihr CEO, ein Mitarbeiter oder ein Bankvertreter sein. Statt auf die Nachricht zu reagieren, wählen Sie eine andere Kommunikationsmethode, wie ein Telefongespräch, um sicherzustellen, dass die Nachricht von dieser Person kommt.
- Achten Sie auf Warnsignale für den Identitätsdiebstahl und informieren Sie Ihre Kreditkartenfirma über mögliche Betrugsversuche.

Die beste Lösung ist die Prävention. Schützen Sie sich vor dem Phishing, indem Sie diesen Richtlinien folgen:

- Nicht auf verdächtige Links klicken
- Sehen Sie sich die Zeichen in der URL genau an. Falls Ihnen die URL verdächtig vorkommt, kopieren Sie diese in einen Unicode-kompatiblen Editor und suchen Sie effektiver nach Punycode-Angriffen.
- Achten Sie auf Nachrichten, die angeblich von großen Technologie-Marken stammen. Prüfen Sie, ob die Nachricht in Hinsicht auf Stil, Vokabular und regionalem Dialekt passt.
- Geben Sie Ihre Kreditkartendaten nicht bei unbekannten oder nicht vertrauenswürdigen Diensten ein
- Wenn ein Link Sie auf Ihre Bank-Website verweist, öffnen Sie Ihre Bank-Website in einem separaten Fenster, indem Sie den Namen manuell eingeben oder die offizielle App verwenden
- Lassen Sie sich nicht von offensichtlichen Tricks hereinlegen, wie dass Sie einen Preis gewonnen haben
- Prüfen Sie die Adressleiste auf verdächtige oder imitierte URLs wie z. B. my.apple.pay.com



Über diese Studie:

Wir wollten den Status des Phishings auf Mobilgeräten und die Informationen besser verstehen, die am meisten gefährdet sind. Die Informationen und Statistiken in diesem Dokument sind das Ergebnis unserer Analyse der Phishing-Trends bei einer Stichprobe von 500.000 Geräten in 90 Ländern aus dem Kundenstamm von Wandera, einer Tochterfirma von Jamf über einen Zeitraum von 12 Monaten. Diese Analyse wurde im 3. Quartal 2021 durchgeführt. Die dabei analysierten Metadaten stammen von aggregierten Protokollen, die keine personenbezogenen oder Organisationen identifizierenden Informationen enthalten.

Mit dieser Analyse wollen wir Ihnen nicht Angst machen, sondern Sie und Ihre Anwender über die verfügbaren Optionen informieren, mit denen Sie alle Aspekte der Geräte-, Benutzer- und Organisationsdaten sichern können. Kontaktieren Sie uns, um zu erfahren, wie Sie Sicherheitsvorkehrungen einsetzen und Ihren Sicherheitsstatus skalieren können.

Erfahren Sie mehr darüber, wie
Jamf bietet vollständige, speziell entwickelte Lösungen, um Unternehmen vor kriminellen Akteuren zu schützen - und gleichzeitig die Nutzererfahrung nur minimal zu beeinträchtigen. Fordern Sie eine Testversion an, um zu sehen, wie der Schutz funktioniert.

Testversion anfordern