

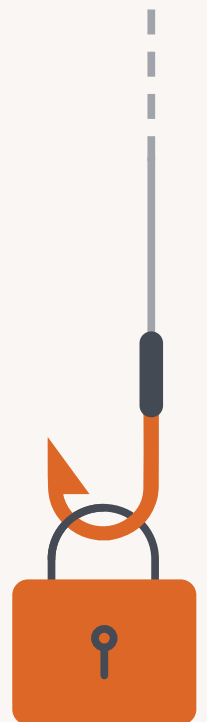
Phishing-Trends Bericht 2021

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 da. Organisationen müssen sie nicht mehr nur auf Desktops und Mobilgeräten, sondern auf sämtlichen Plattformen bekämpfen.

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 besonders wertvoll, 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 längst über schlecht formulierte E-Mails hinaus entwickelt, die „nicht beanspruchte Lotteriegewinne“ anbieten. Die Attacken sind jetzt nicht nur besser personalisiert und damit überzeugender, sie erreichen die Benutzer auch an mehr Orten als je zuvor. Die Angreifer zielen nicht nur auf Verbraucher ab, sondern wollen auch Passwörter und Daten von Unternehmen erbeuten. Das liegt nicht zuletzt an der zunehmenden Akzeptanz von Mobilgeräten..



Phishing-Angriffe täuschen eine zunehmende Anzahl von Nutzern mobiler Geräte

Der Großteil des Datenverkehrs im Web wird mittlerweile von Nutzern mobiler Geräte verursacht. 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. Da viele Anwender Mobilgeräte unterwegs nutzen, lassen sie sich leichter ablenken. Das Gefühl, ein persönliches Gerät zu nutzen, gibt den Mobilgerät-Nutzern eine vermeintliche Sicherheit. Beide Faktoren begünstigen Angriffe zusätzlich.

Die Angreifer produzieren immer überzeugendere Phishing-Seiten, um auf Nutzer von Mobilgeräten abzielen. Bereits einer von zehn Nutzern fallen auf Phishing-Angriffe herein. Das bedeutet, dass man Nachrichten nicht nur empfängt, sondern tatsächlich auf sie klickt.

Unten stehende Grafik zeigt einen Zuwachs von 160 Prozent bei der Zahl der Mobilgerät-Benutzer, die in den vergangenen zwölf 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 vertrauenswürdige 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

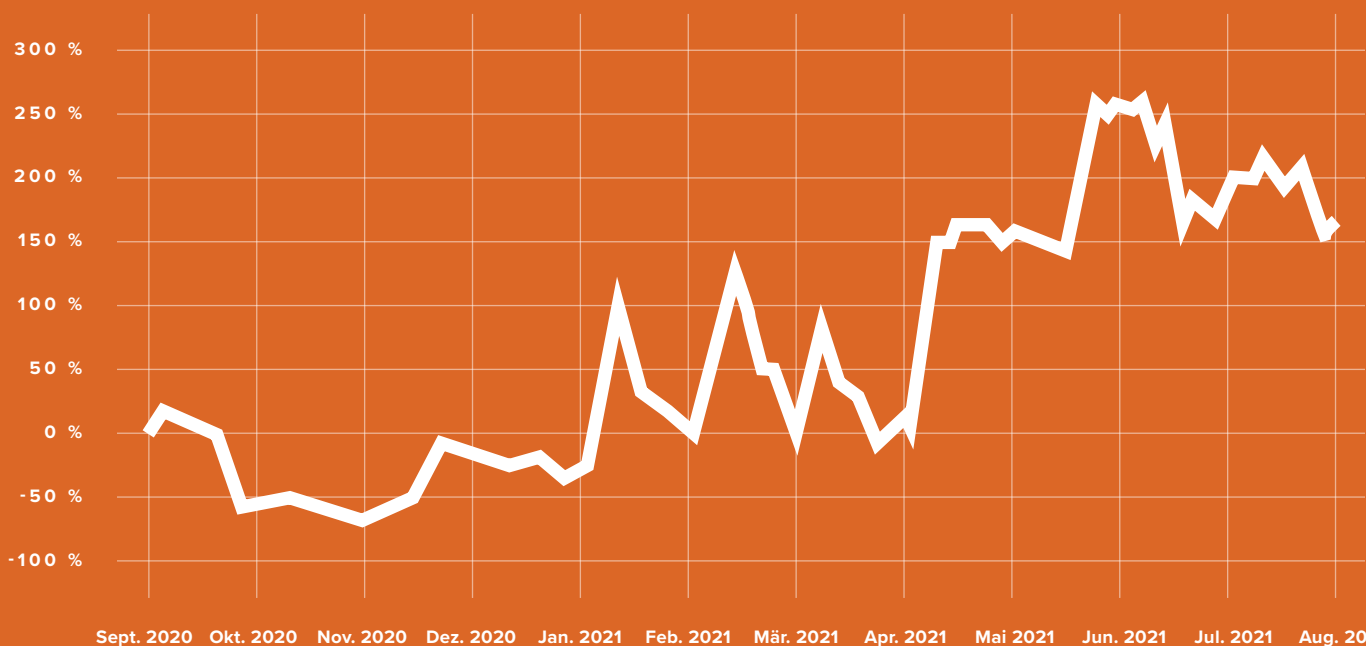
Quelle: Wandera, eine Tochterfirma von Jamf

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

Quelle: Wandera, eine Tochterfirma von Jamf

PROZENTUALER ZUWACHS

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 tragbaren 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, die häufig in Textnachrichten verwendet werden, verbergen die vollständige Domain.

Anwender erwarten nicht, dass Phishing immer öfter außerhalb von E-Mails passiert

Bisher wurde Phishing in Unternehmen als Sicherheitsproblem betrachtet, das ausschließlich E-Mails betraf. Daher wurde die Lösung nicht in das Gerät, sondern in das E-Mail-Programm integriert. In dem Maße, wie Leute zunehmend mobil arbeiten, verwenden sie (1) mehr Apps, die nicht geschützt sind, und (2) befinden sich außerhalb des Firmennetzwerkes und profitieren daher nicht von den Schutzmaßnahmen im Firmengelände.

Geräte für Endanwender bieten immer öfter eine konsolidierte Kommunikationsplattform, auf der eine Vielzahl von Messaging- und Social-Media-Apps mit In-App-Direktnachrichten genutzt werden können. MacBooks mit Apple Silicon-Prozessoren 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-Symbol ist nicht länger ein Garant für Sicherheit

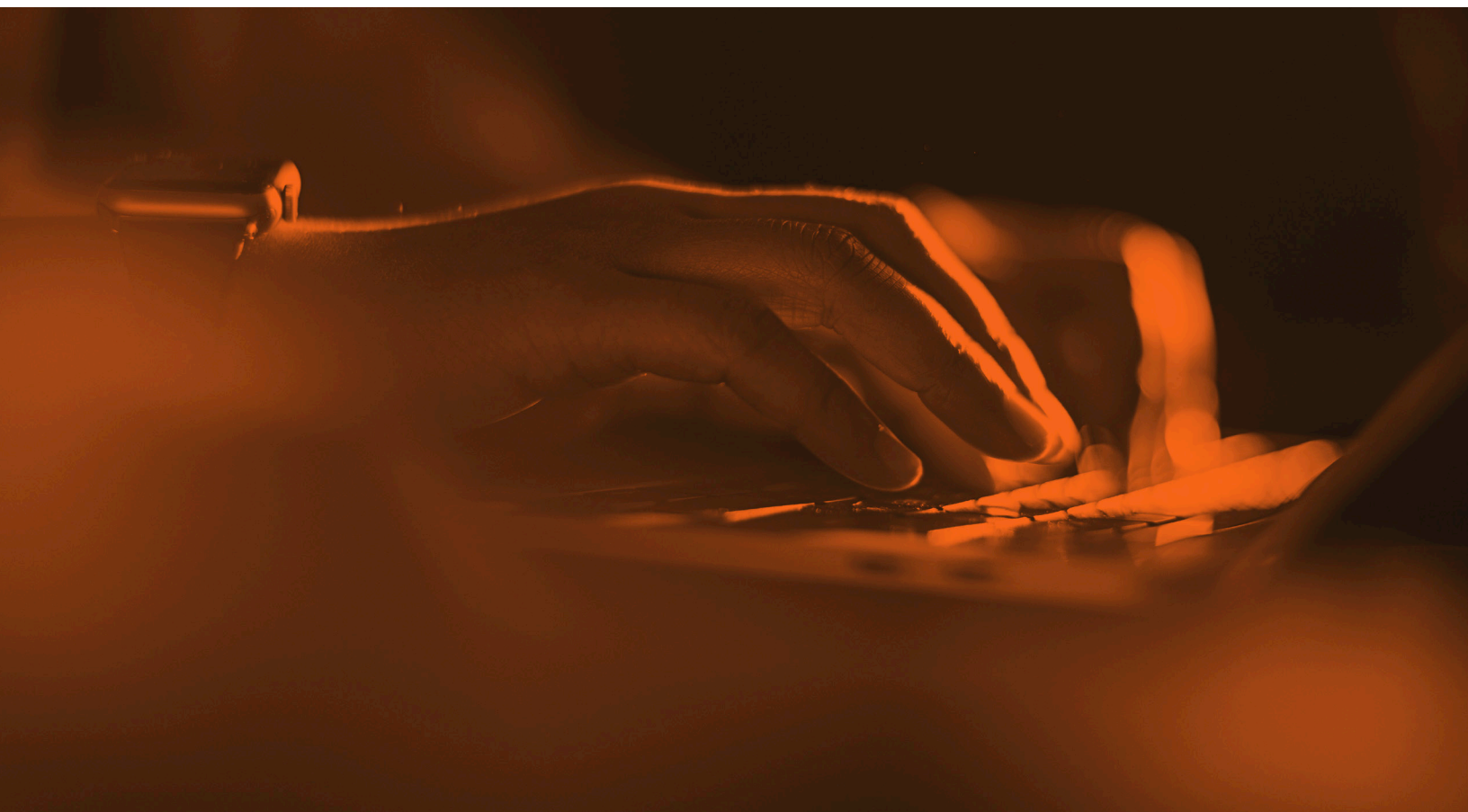
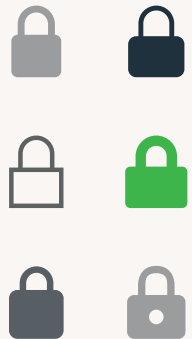
Eine doppelte Überprüfung der Adressleiste, ob ein Vorhängeschloss vorhanden ist, war früher eine einfache Möglichkeit, eine gefährliche Domain zu erkennen. Nun können Angreifer zahlreiche kostenlose Dienste nutzen, um schnell und mühelos eine SSL-Zertifizierung für bösartige Phishing-Websites zu erhalten. 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 es sie nun nichts mehr kostet, ist es für Angreifer besonders lukrativ, ihre Phishing-Websites mit einem SSL-Zertifikat auszustatten.

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 kriminellen Absichten zu verbergen. Unseren Daten zufolge ist diese Zahl 2018 deutlich auf einen Wert von 65 Prozent 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 Benutzern über den Browser vorgetäuscht, dass sie mit einer Website kommunizierten, obwohl sie tatsächlich mit einer anderen Website kommunizierten. Unicode-Zeichen erzeugen Domainnamen, die dem bloßen Auge vertraut vorkommen, aber in Wirklichkeit auf einen anderen Server verweisen oder auf 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?

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.



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://google.com>

xn--googe-95a.com

Starbucks

 <https://starbucks.com>

xn--starucks-hpd.com

Rolex

 <https://rolex.com>

xn--rolx-nu5a.com

Paypal

 <https://t.paypal.com>

t.xn--ayal-9ndc.com

Facebook

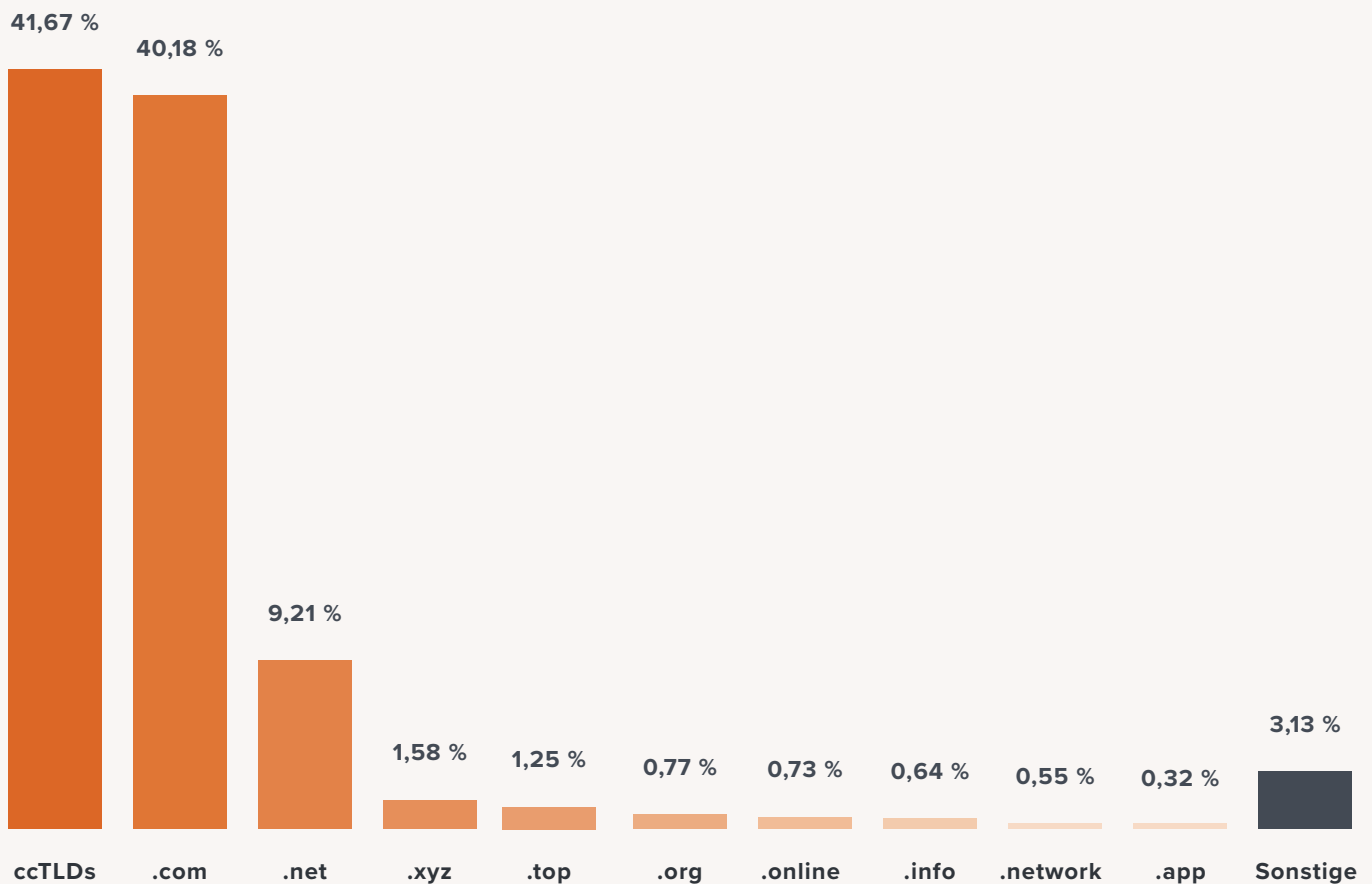
 <https://www.facebook.com/login.en.do>

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 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

Fazit: Werden Vorhängeschloss, Punycode und ungewöhnliche TLDs zusammen verwendet, ist es sehr leicht, eine überzeugende Phishing-Domain zu erstellen, die auch mit den größten Marken verwechselt werden kann.



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. Menschen werden eher einem Phishing-Angriff zum Opfer fallen, wenn der Köder für eine Website ausgelegt 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 Ebenen von persönlichen und geschäftlichen Daten. Dabei sind nicht diese Unternehmen schuld. Sie werden lediglich benutzt, da jeder sie kennt und sie deshalb kriminellen Akteuren eine hohe Chance bieten, an wertvolle Informationen zu kommen.

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. Der Fehler eines Mitarbeiters, der Ziel eines cleveren Phishing-Angriffs wird (in dem er beispielsweise die Anmeldedaten für Google Drive bestätigen soll), kann einem Hacker den Zugriff zu Unternehmensdaten in diesen beliebten Cloud-Anwendungen verschaffen..

Unseren Untersuchungen zufolge sind die drei führenden Marken in Phishing-Angriffen, mit denen Benutzer 2020 und 2021 dazu gebracht wurden, auf Phishing-Links zu klicken, Apple, PayPal und Amazon, die für 43 %, 27 % und 9 % der jeweiligen Angriffe verwendet wurden.



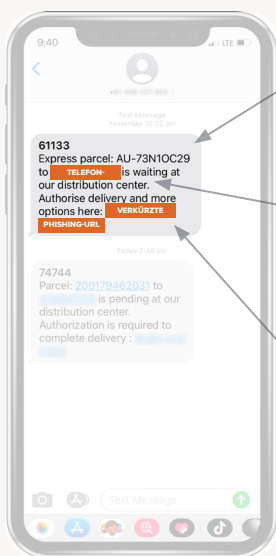
Die 10 häufigsten Marken in Phishing-Kampagnen im Jahr 2021

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

Australia Post - eine erfolgreiche Phishing-Kampagne im Fokus

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). Dies war ein opportunistischer Angriff, da sich viele Menschen in Australien während der strengen und wiederholten COVID-19 Lockdowns auf die Lieferung nachhause 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.



DRINGENDE EINTREFFENDE NACHRICHT DRÄNGT OPFER ZUR NÄCHSTEN PHASE DES ANGRIFFS

VERWENDUNG DER TELEFONNUMMER IN DER NACHRICHT ZUR PERSONALISIERUNG DES ANGRIFFS

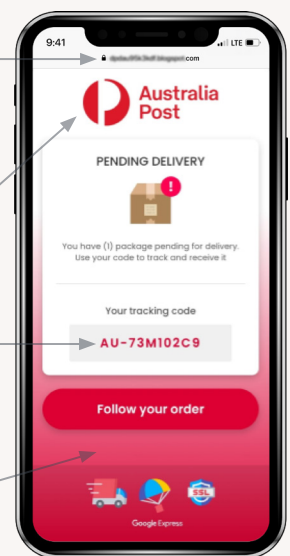
GEKÜRZTE URL ZUR VERSCHLEIERUNG DER VOLLSTÄNDIGEN DOMAINS

VERWENDUNG DES VORHÄNGESCHLOSS-SYMBOLS (HTTPS/SSL-ZERTIFIKAT) UM DEN EINDRUCK EINER SICHEREN WEBSITE ZU ERWECKEN

VERWENDUNG DES OFFIZIELLEN MARKENLOGOS

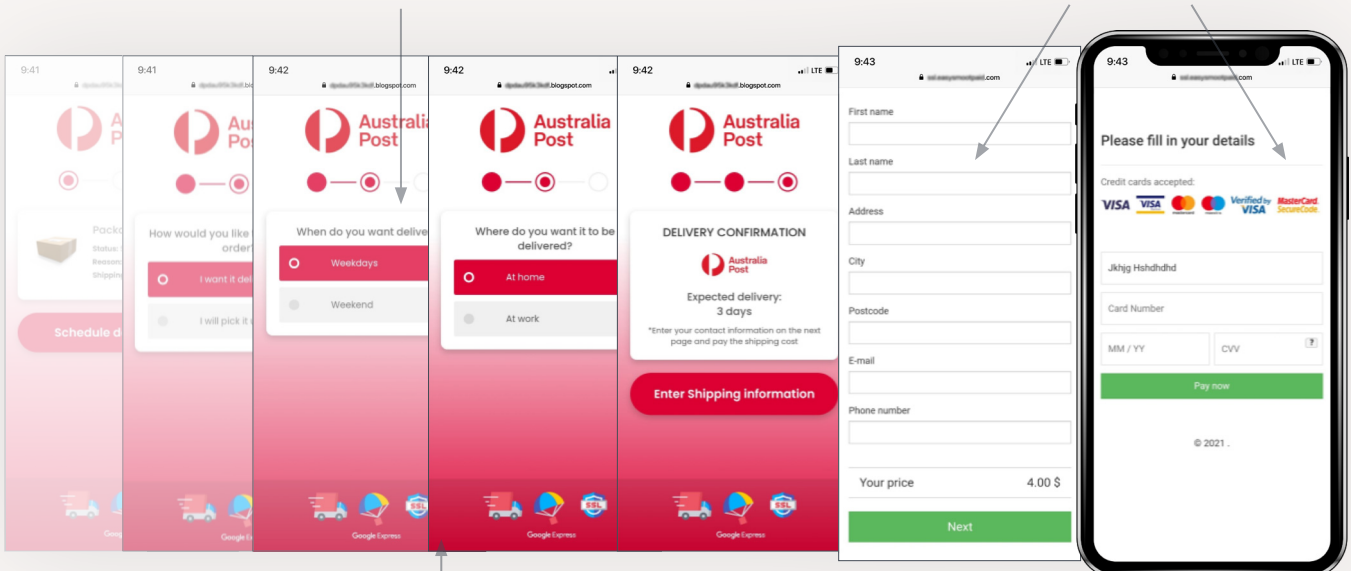
DIE VERWENDUNG DES GLEICHEN TRACKING-CODES, DER IN DER NACHRICHT WAR, BRINGT OPFER ZUR NÄCHSTEN PHASE DES ANGRIFFS

VERWENDUNG DER MARKENFARBEN



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 von Phishing. Erstens verwendet die URL nicht die 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 verlangt, 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. edenkt man die Anzahl der möglichen Top-Level-Domains 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, die nicht nur für E-Mails sondern über alle Kommunikations-Apps hinweg funktioniert, entscheidend. Damit können sowohl die bekannten Formen von Attacken gestoppt werden, also auch die anspruchsvolleren Angriffe, die auf Unternehmen als ganzes abzielen.

Sie wurden 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:

- Klicken Sie nicht auf verdächtige Links.
- 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 Punycode-Angriffe schneller auszumachen.
- Achten Sie auf Nachrichten, die angeblich von großen Technologie-Marken stammen. Prüfen Sie, ob die Nachricht in Hinsicht auf Stil, Vokabular und regionaler Schreibweise passt.
- Geben Sie Ihre Kreditkartendaten nicht bei unbekanntem oder nicht vertrauenswürdigen Diensten ein
- Wenn ein Link Sie auf Ihre Bank-Website weiterleiten, öffnen Sie Ihre Bank-Website in einem separaten Fenster, indem Sie den Namen manuell eingeben oder die offizielle App verwenden.
- Lotteriegewinn, Erbschaft & Co: Fallen Sie nicht auf offensichtliche Tricks herein.
- Prüfen Sie die Adressleiste auf verdächtige oder imitierte URLs wie z. B. my.apple.pay.com.



Über diese Studie:

Wir haben den Status von Phishing auf Mobilgeräten untersucht, um besser zu verstehen, welche Informationen am meisten gefährdet sind. Die Informationen und Statistiken in diesem Dokument sind das Ergebnis unserer Analyse von Phishing-Trends. Die Stichprobe betrug 500.000 Geräte in 90 Ländern über einen Zeitraum von zwölf Monaten. Die Nutzer der Geräte stammen aus dem Kundenstamm von Wandera, einer Tochterfirma von Jamf. 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 nicht Angst machen, sondern Sie über die verfügbaren Optionen informieren, mit denen alle Aspekte der Geräte-, Benutzer- und Organisationsdaten gesichert werden können. Kontaktieren Sie uns, um zu erfahren, wie Sie Sicherheitsvorkehrungen einsetzen und Ihren Sicherheitsstatus skalieren können.

Erfahren Sie mehr

Jamf und Threat Defense bieten eine vollständige, speziell entwickelte Lösung, um Apple-Benutzer vor kriminellen Akteuren zu schützen – und gleichzeitig die Nutzererfahrung nur minimal zu beeinträchtigen. Oder fordern Sie eine Testversion an, um zu sehen, wie Benutzer geschützt werden können.

[Testversion anfordern](#)