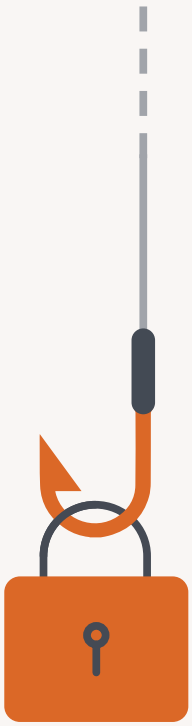
Phishing Trends Report 2021

In 2021, phishing has infiltrated every form of communication, from work and personal e-mail to SMS, social media, and even advertising.

Social engineering that was once isolated to corporate email has become the most damaging cybersecurity threat facing organizations today, across all platforms — desktop and mobile included.

Why? Because it's easier for an attacker to exploit a person and capture data via a phishing attack than it is to exploit a robust device operating system. In fact, user credentials are far more valuable to an attacker in this age of cloud-enabled enterprises, as they provide access to sensitive data that is stored and managed beyond the device in SaaS applications, online file storage repositories and data centers.

Phishing attack delivery has evolved far beyond poorly-worded emails offering 'unclaimed lottery winnings.' They are not only more personalized and more convincing, they are reaching users in more places than ever before and increasingly going beyond consumers to target business credentials and data. This is largely due to the adoption of mobile.



Phishing attacks are fooling an increasing number of mobile users

Most web traffic is now associated with users who are mobile. Therefore, it doesn't come as a shock that hackers use this to their advantage by crafting attacks specific to mobile platforms. Mobile devices have smaller screens and feature a number of visual shortcuts, meaning spotting suspicious URLs or malicious senders is far more difficult than on desktop. Users are also more distracted and vulnerable on mobile devices due to their portable nature and inherently personal feel.

Attackers continue to produce ever more convincing phishing sites, that target mobile users, with as many as 1 in 10 mobile users falling for phishing attacks. This doesn't mean simply receiving messages, but actually clicking on them.

The below graph shows a 160% increase in mobile users falling victim to phishing over the past 12 months. This isn't reflective of the volume of attacks present online but rather the rate at which people are falling for them. This increase in people taking the bait is likely due to attackers evolving their techniques. They are now using trusted apps to deliver them, they are registering compelling domains, and imitating well-known brands to reach more users with less investment.

1 in 10

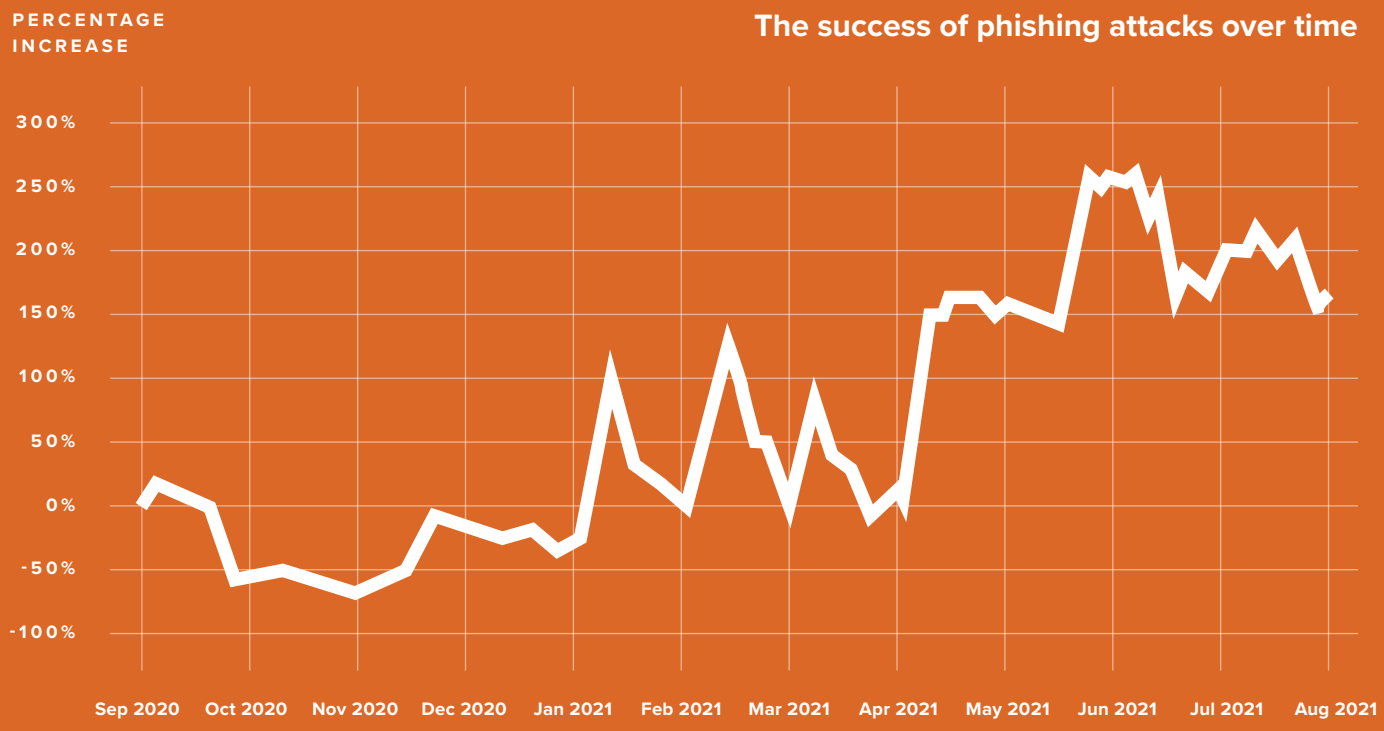
people click on phishing links while on their mobile devices

Source: Wandera, a Jamf Company

The number of mobile users falling for phishing attacks has increased by 160% YoY

Source: Wandera, a Jamf Company

The success of phishing attacks over time



Source: Wandera, a Jamf Company

Phishing attacks are harder to spot on portable devices

Todays highly portable devices, used for remote work, make phishing harder to detect.

- An increased use in mobile devices results in smaller screen sizes which leaves less space to evaluate the legitimacy of a website.
- User interface design improvements have led to design decisions that typically hide the already tiny address bar as the user scrolls down to make room for page content.
- Distracted users working across multiple devices and communicating and collaborating over a wide variety of apps, tend to rush through various pages and notifications. Additionally, many app developers choose to highlight the “Accept” or “OK” button in prompts, leading users down a path of automatically accepting prompts without review.
- Streamlined visuals that prioritize screen real estate for content vs. metadata prevent the user from seeing or evaluating the link destination before clicking.
- URL shorteners such as Bitly or Owly – commonly used in text messages – hide the full domain.

Phishing is being delivered outside of email, where people aren’t expecting it

Traditional security approached phishing as a corporate email problem. They put the solutions in the email appliance itself instead of on the device. As people went mobile, they (1) started using more apps, which were not protected; and (2) were outside the perimeter and, therefore, did not benefit from any of the protections built around the physical campus.

End user computing devices are increasingly offering a consolidated communications platform — where you can have a lot of messaging and social media apps with in-app direct message. MacBooks using Apple silicon can run not only macOS apps, but also iOS apps, and Windows, etc., to offer a cohesive compute experience. Messaging apps tend to be an overlooked area in the organization’s defenses, and therefore appealing for attackers.

Focusing on mobile has allowed hackers to move on from the trusted domain of email, and onto a multitude of new distribution methods such as SMS, WhatsApp, Messenger, Instagram and LinkedIn, services that users trust.





The padlock is being used to deceive users further

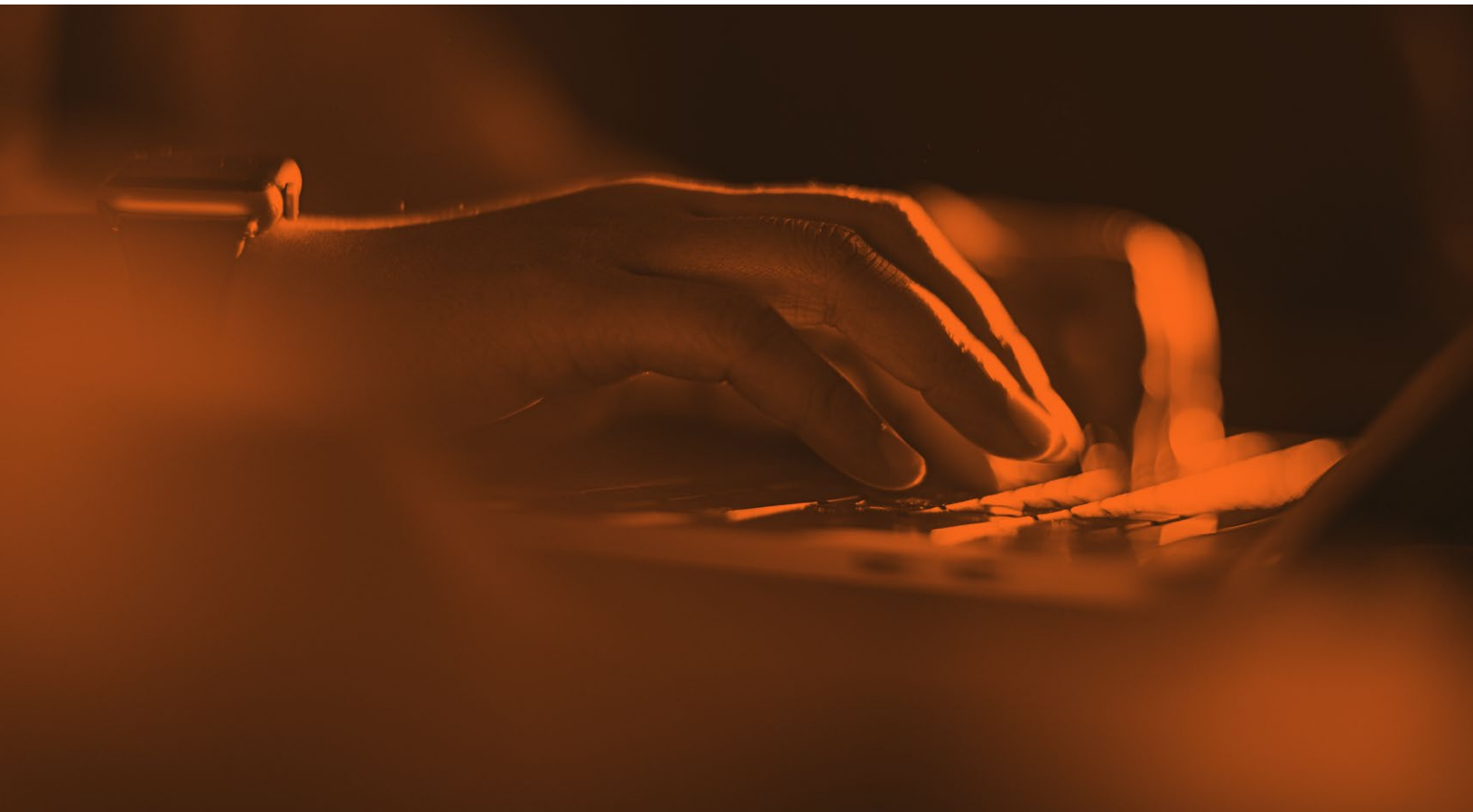
Double-checking the address bar for a padlock used to be an easy way to catch a bad domain, but now there are a multitude of free services online that attackers can use to quickly and easily gain SSL certification for malicious phishing sites. Unfortunately, this is effective because users believe the padlock symbol preceding a URL is a reliable indicator that a website is safe. With the cost barrier removed, there's no reason why an attacker wouldn't encrypt their bad sites.

93% of phishing domains that are hosted on a "secure" website with a padlock in the URL bar

Source: Wandera, a Jamf Company

Today, 93% of successful phishing sites are utilizing HTTPS verification to conceal their deceitful nature. According to our data, that number has increased dramatically from 65% in 2018.

Source: Wandera, a Jamf Company



Punycode makes bad domains harder to identify

Attackers are increasingly using punycode to make their phishing domains harder to detect. Punycode converts words that use unicode characters (in alphabets like Cyrillic, Greek and Hebrew, for example) into ASCII characters so that computers can understand them.

The origins of punycode attacks date back to when browsers didn't support unicode and only used ASCII to display URLs; attackers started using these character sets because they could register domains that looked very similar to existing/trusted domains and the browser could ultimately be used to fool the user into believing they were communicating with one site when, in fact, they were communicating with another. Unicode characters make domain names that look familiar to the naked eye but actually point to a different server or link to an unfamiliar domain.

According to our data, over the past 12 months, 2% of successful zero day phishing attacks contained punycode. Below are some examples. Can you spot the unicode characters in the below domains?

2% of phishing attacks that users fell victim to contained punycode

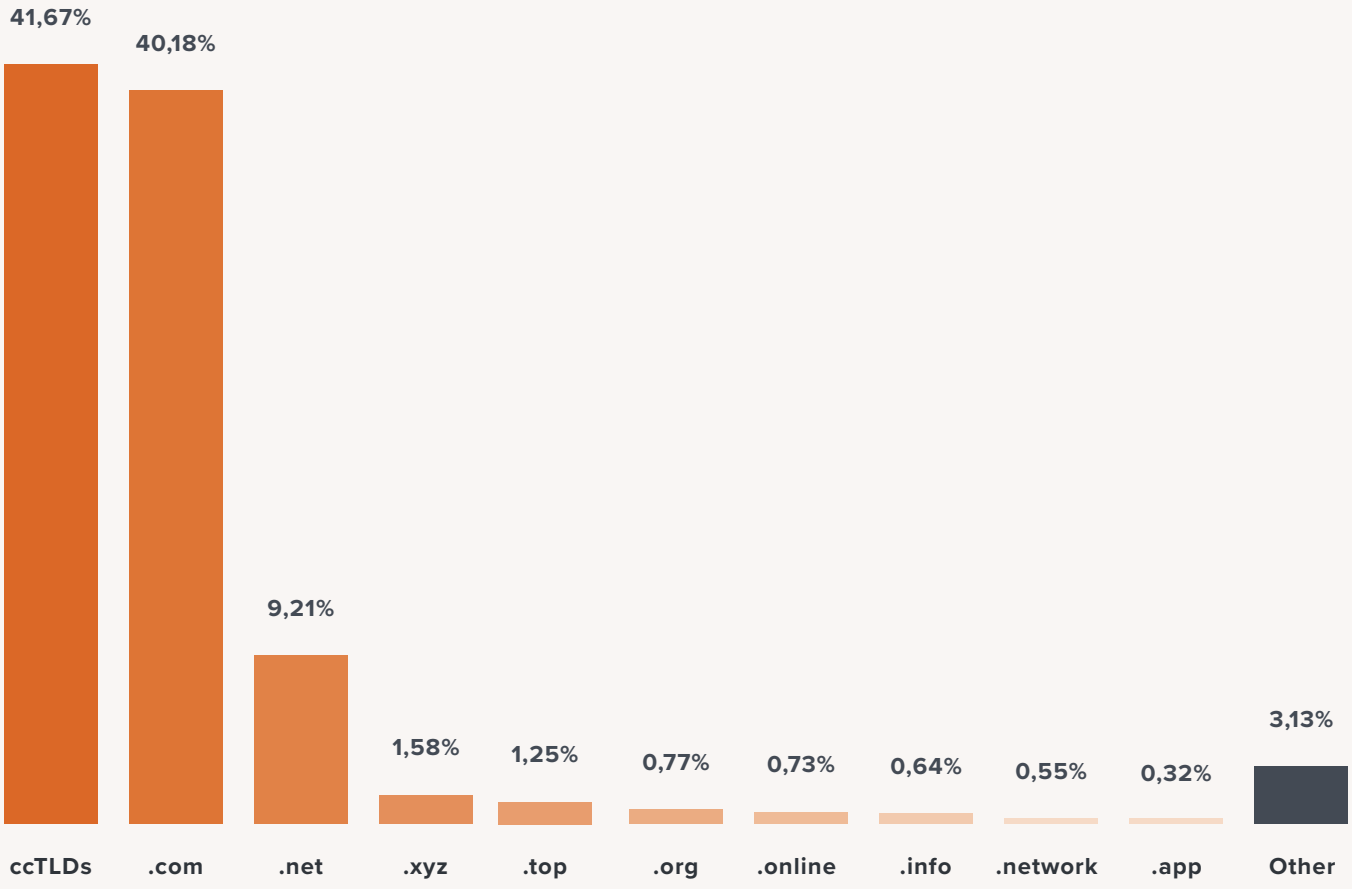
Source: Wandera, a Jamf Company

BRAND	WHAT THE USER SEES (UNICODE)	THE "DECODED" 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

Obscure Top Level Domains are making matters worse

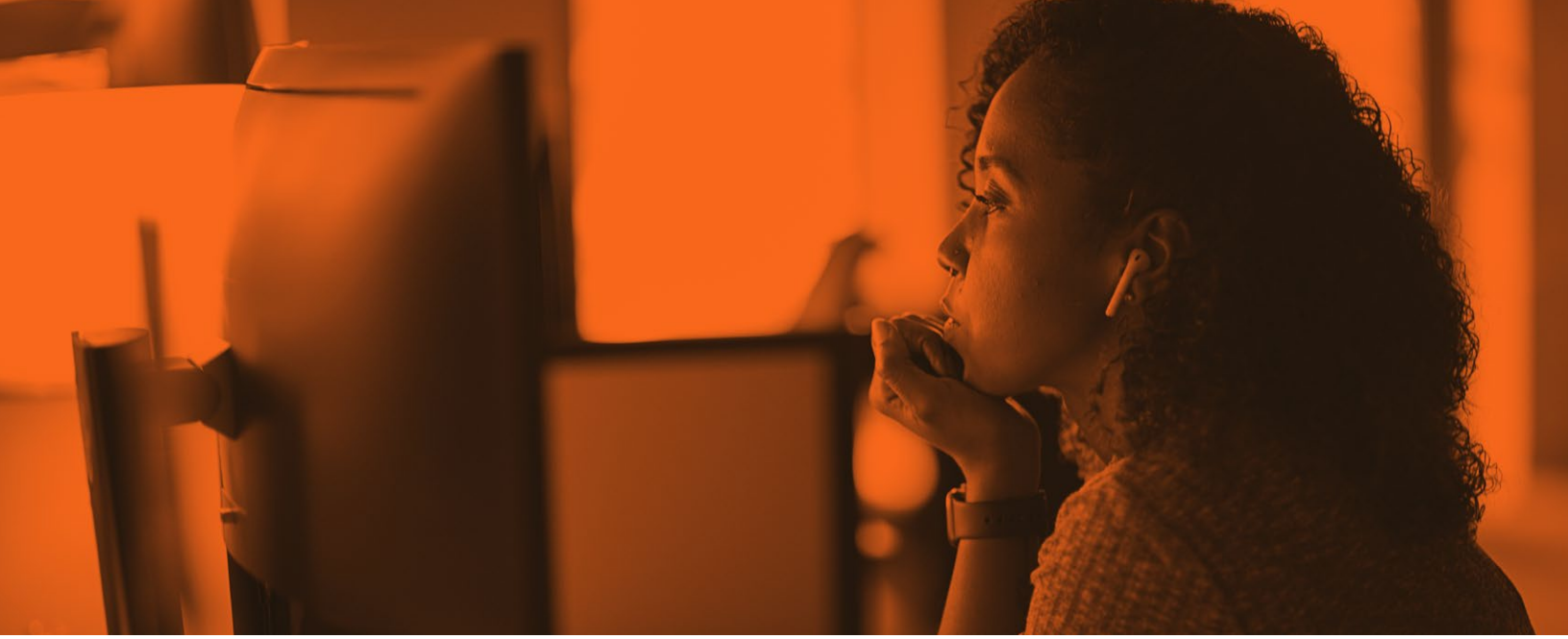
Top Level Domains (TLD) used to be mainly just .com, .net, .org, etc. In recent years, more domains using different country code top level domains (ccTLD) and businesses-specific TLDs, (eg. .attorney, .technology, .airline) have begun popping up. Below is the share of top level domains we have seen in successful phishing attacks. The danger here is that users might see a brand name they recognize, but with a TLD that isn't the usual one. For example, a hacker might register microsoft.xyz to host a Microsoft-themed phishing attack, and when it gets discovered, replace it with microsoft.info or microsoft.network, and so on.

Below is the share of TLDs used in successful phishing attacks detected on our platform in the past 12 months. The common .com and .net TLDs are the most popular, along with a consolidation of ccTLDs such as .ru, .uk, and .co.



Source: Wandera, a Jamf Company

Key takeaway: When you add the padlock, punycode and unconventional TLDs together, you can see how easy it is to make a convincing phishing domain that imitates even the biggest brands.



Top 10 brands used in successful phishing attacks

To increase the success rate of an attack, malicious actors need to be selective when deciding which companies to impersonate.

Attackers are moving away from regional attacks (e.g., using a local bank's brand) to those that incorporate global, tech-oriented brands. People are more likely to fall victim to a phishing attack when the bait is for a site they actually have an account with. As single-sign on technology is incorporated into more and more apps, credentials for large influential companies such as Apple, Google, Amazon, Microsoft, etc. provide access to more than just email... they are the "keys to the kingdom" and open up more layers of personal and business data. It's not these companies that are at fault, they are simply used by the malicious actors because they are recognizable and considered rich sources of valuable information.

Malicious actors are increasingly targeting applications used for work, such as Office 365 and Google's G Suite apps. As businesses strive to move their corporate assets to the cloud, this is a major concern. One slip up by an employee who receives a clever phishing attack (e.g., asking them to confirm their Google Drive login credentials) can give a hacker access to corporate assets stored on these types of popular cloud applications.

According to our research, the top three brands used in phishing attacks that were successfully used to trick users into actioning the phishing link in 2021 are Apple, PayPal and Amazon, which account for 43%, 27% and 9% of those attacks respectively.

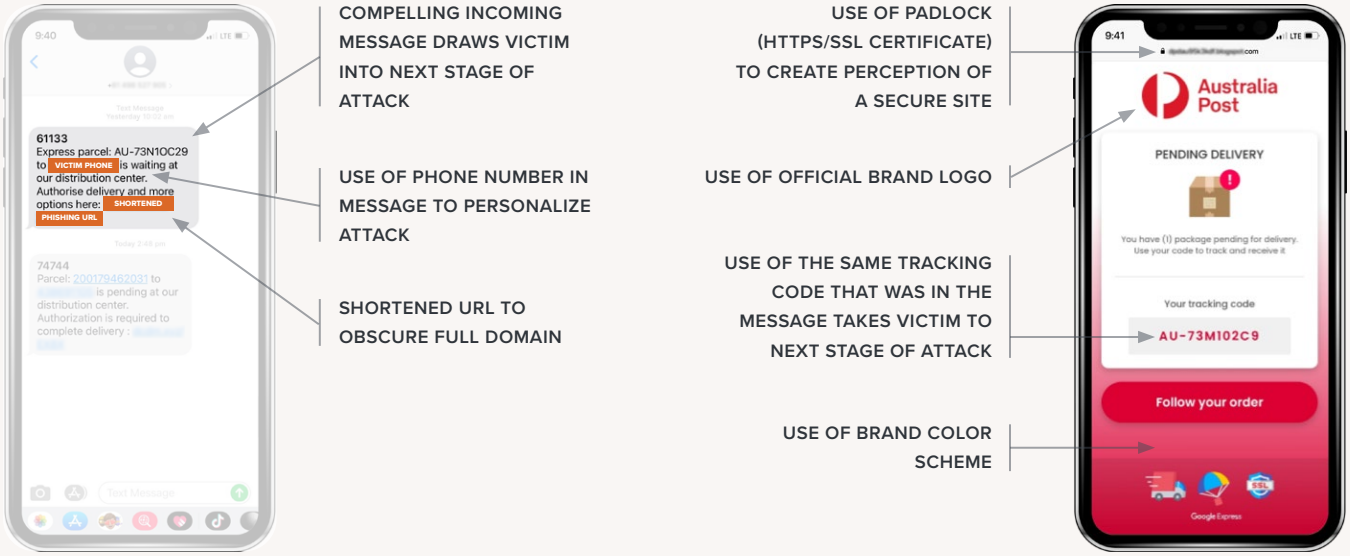
Top 10 brands used in phishing campaigns in 2021

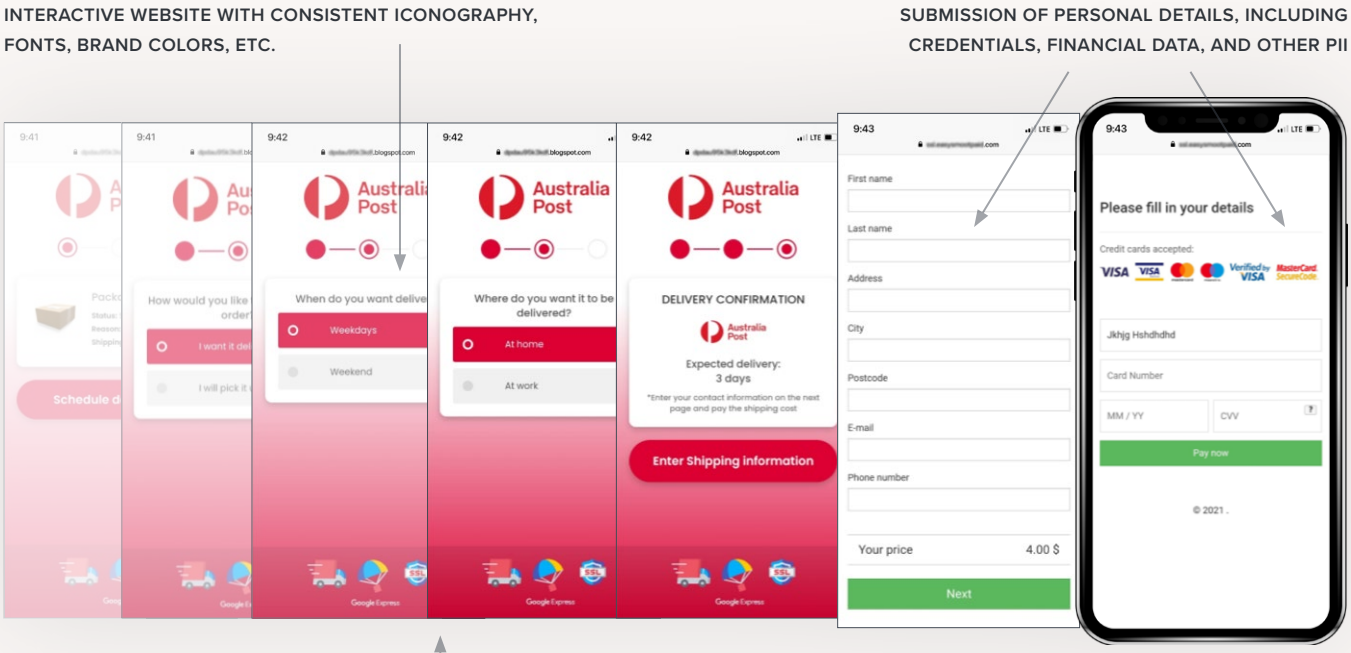
1. **Apple**
2. **PayPal**
3. **Amazon**
4. **Chase**
5. **Facebook**
6. **Google**
7. **Twitter**
8. **Netflix**
9. **Microsoft**
10. **Wells Fargo**

Source: Wandera, a Jamf Company

Phishing campaign spotlight — Australia Post

Our researchers investigated a phishing campaign when multiple suspicious text messages were reported. The messages were themed around package delivery, using the well-known Australia Post brand (Australia Post is the equivalent of the USPS in the US or Royal Mail in the UK so the pool of potential victims is anyone that lives in Australia and receives mail). An opportunistic attack given how much people were relying on home delivery during Australia's strict and repeated COVID-19 lockdowns. Like the other major brands being used in phishing attacks, Australia Post hasn't done anything wrong, the brand is simply being used by attackers because of the recognizable name.





Source: Wandera, a Jamf Company

There are many poorly built phishing campaigns out there. Sometimes the message doesn't even correlate to the page content, or the page content is a very generic scam. The Australia Post phishing attack is a little more sophisticated, given there is continuity between the message and the page content to trick the victim into believing they need to authorize a package delivery.

Although this is a well-executed attack, there a few obvious signs of a phish here. First, the URL does not use the auspost domain. Second, the branding is convincing, but it's not a perfect match with the legitimate Australia Post website. Third, the user is redirected to another off-brand domain which asks for payment when payment wouldn't typically be needed to authorize a delivery. Finally, Australians spell center 'centre'; the smallest details can give away a phishing attack so keep a sharp eye!

A quick reality check

Many phishing sites are published online for only a few hours before hackers move to an entirely new hosting server. This allows them to evade detection and maintain ongoing campaigns without being blocked. The risk to users is highest in those first critical hours before static, list-based threat intelligence is updated.

In the Australia Post attack above, when the phishing domain is reported and taken down, all the attacker needs to do is register a new domain and relaunch the attack, until that new domain is reported too, and they repeat. When you think about the number of top level domains out there, and the many subdomains we see in legitimate URLs now (such as login., mobile., or en., it's easy to see how an attacker can keep a campaign like this alive. Mix and match and build your own phishing URL with just a few examples below and then ask yourself, would you take the bait if you saw it?

Always remember:

In these situations when you receive a convincing message we recommend going straight to your service's app or website rather than clicking through from an email or message.

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

Recommendations

Phishing attacks exploit the most vulnerable part of an organization: its employees. Employees are often a corporation's most valuable asset, but when it comes to keeping data safe they double up as their biggest security weakness.

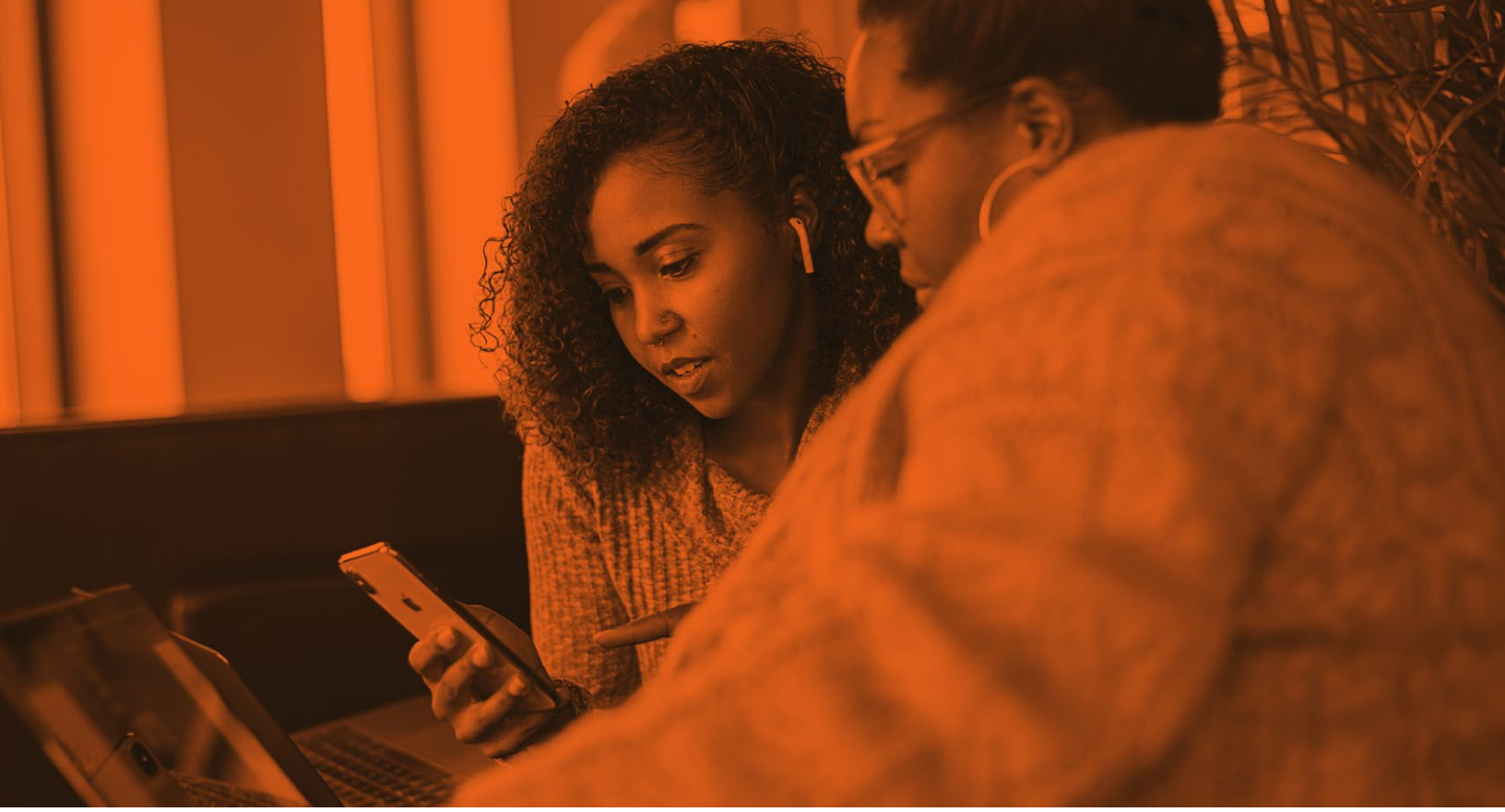
That's why a zero-day phishing solution – specifically one that operates across all communication apps, not just email – is critical in stopping both the common attacks and the more sophisticated ones that are being launched against your business.

So you've been phished, now what?

- Change all your passwords for the accounts that have been compromised as well as the accounts that use the same or similar passwords to those that have been captured by the hacker.
- If you entered your credit card information in the phishing page, cancel your card.
- Take your computer offline or delete your email account to avoid spreading phishing links to your contact lists.
- Contact the company or person that was imitated in the attack – it might be your CEO, coworker, or bank representative. Rather than responding to the message, choose a different communications method, such as a phone call, to verify it was them.
- Watch out for warnings of identity theft and put a fraud alert on your credit account.

The best remedy is prevention. Stay safe from phishing by following this guidance:

- Don't click on suspicious links
- Look closely at the characters in the URL. If suspicious, copy the URL from your browser into a unicode compatible editor to more effectively look for punycode attacks
- Be aware of messages claiming to be from the big tech brands. Check if the message is consistent with their tone, vocabulary, regional dialect, etc
- Don't enter your credit card information into unknown or untrusted services
- If a link directs you to your banking website, open up your banking site in a separate window by typing the name in manually, or use the official app
- Don't fall for obvious scams that claim you've won a prize
- Check the address bar for suspicious or copycat URLs, for example, my.apple.pay.com



About this research

We wanted to better understand the state of mobile phishing and the information that is most at risk. The information and statistics found in this paper is the result of our analysis of phishing trends within a sample of 500,000 protected devices across 90 countries within the customer base of Wandera, a Jamf company, over a period of 12 months. This analysis was carried out in Q3 of 2021. The metadata analyzed in this research comes from aggregated logs that do not contain personal or organization-identifying information.

Our intention with this analysis is not to invoke fear, but instead educate you and your users on the options available and how best keep all aspects of device, user and organizational data secure. Contact us to learn how you can put safeguards in place and scale your security posture.