Cyberint

THE PHISHING & IMPERSONATION *Protection Handbook*

August 2024

Table of Contents

Introductory Comments

You might think that businesses would be pretty good at protecting against phishing attacks by now. After all, this type of cyber risk has been around for decades, and phishing is not a particularly sophisticated type of attack in a technical sense. It doesn't require threat actors to hack complex systems or write their own software. They mostly just need to master social engineering techniques, such as executive impersonation.

Yet, despite this, phishing attacks remain as prevalent as ever – and are actually getting worse. The frequency of phishing incidents surged by 1,265 percent in 2023, due especially to the advent of generative AI technology – which can "facilitate phishing and social engineering, which enables better intrusion, increased credibility and more damaging attacks," as Gartner notes.

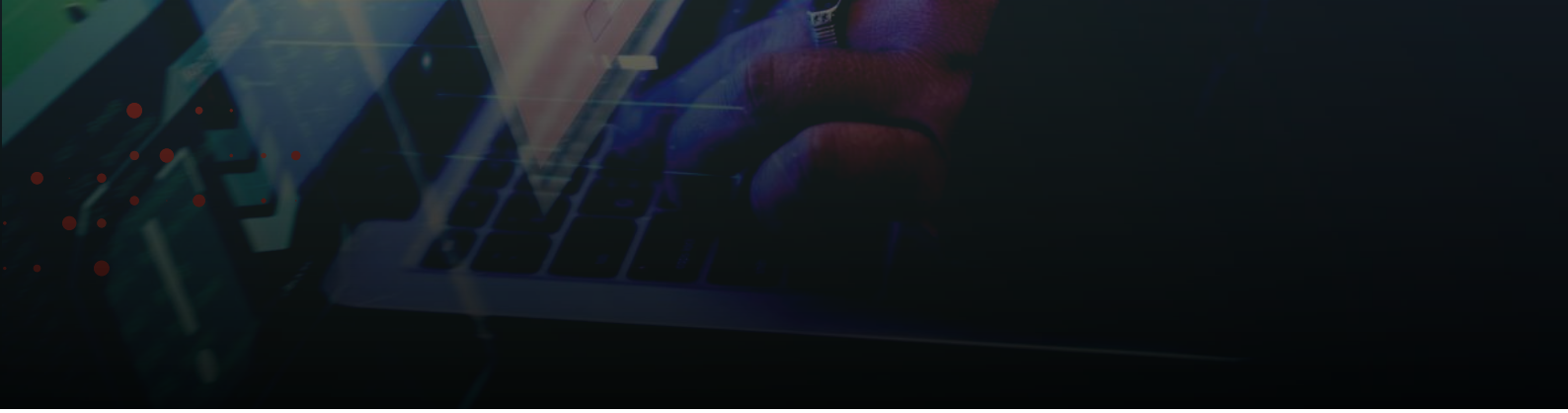
In a sense, it's understandable why companies continue to exhibit such a poor track record of defending against phishing attacks. Humans are a social species, and most of us are naturally inclined to want to trust others. We want to respond and engage with people and brands when they ask for help. By exploiting that tendency via social engineering, threat actors can trick well-meaning people into becoming the weakest link in cyber defenses.

> ***Companies work extremely hard to develop their brand, spending large sums to earn customer confidence and trust, but threat actors exploit that hard earned trust. They impersonate the brand and fool the average customer.***

Indeed, even after completing anti-phishing training, the percentage of targets who fall for phishing scams can be as high as 5 percent. (Without training, it's 32.4 percent.)

That's the bad news. The good news is that, with the right tools and strategies, it's possible to minimize your organization's risk of experiencing a successful phishing attack. Doing so starts with understanding how, and how to protect against the social engineering techniques that threat actors rely on to launch phishing attacks.

This guide provides guidance on these topics by discussing the four main types of phishing impersonation, then offering tips on defending against each one.



Why Do Threat Actors Undertake Phishing Attacks?

Phishing is still one of the top 3 successful attack vectors.

The reason for its success is twofold:

A. It could be relatively simple for a novice threat actor to set up a phishing campaign.

B. It's designed to trick your brain to trust it - which can be achieved fairly easily, especially in the hectic digital life we are living.

The main goal of a phishing campaign is to make money, by here are three common ways of achieving that objective:

Steal Data

Such as valid credentials, credit card numbers, bank account details and other PII that can be used in a future attack.

Steal Funds

Directly from the victim by tricking them into making a payment (for example tax for a package in transit).

Deploy Malware

Via a malicious payload to a device allowing a threat actor to continue further in a cyber attack.

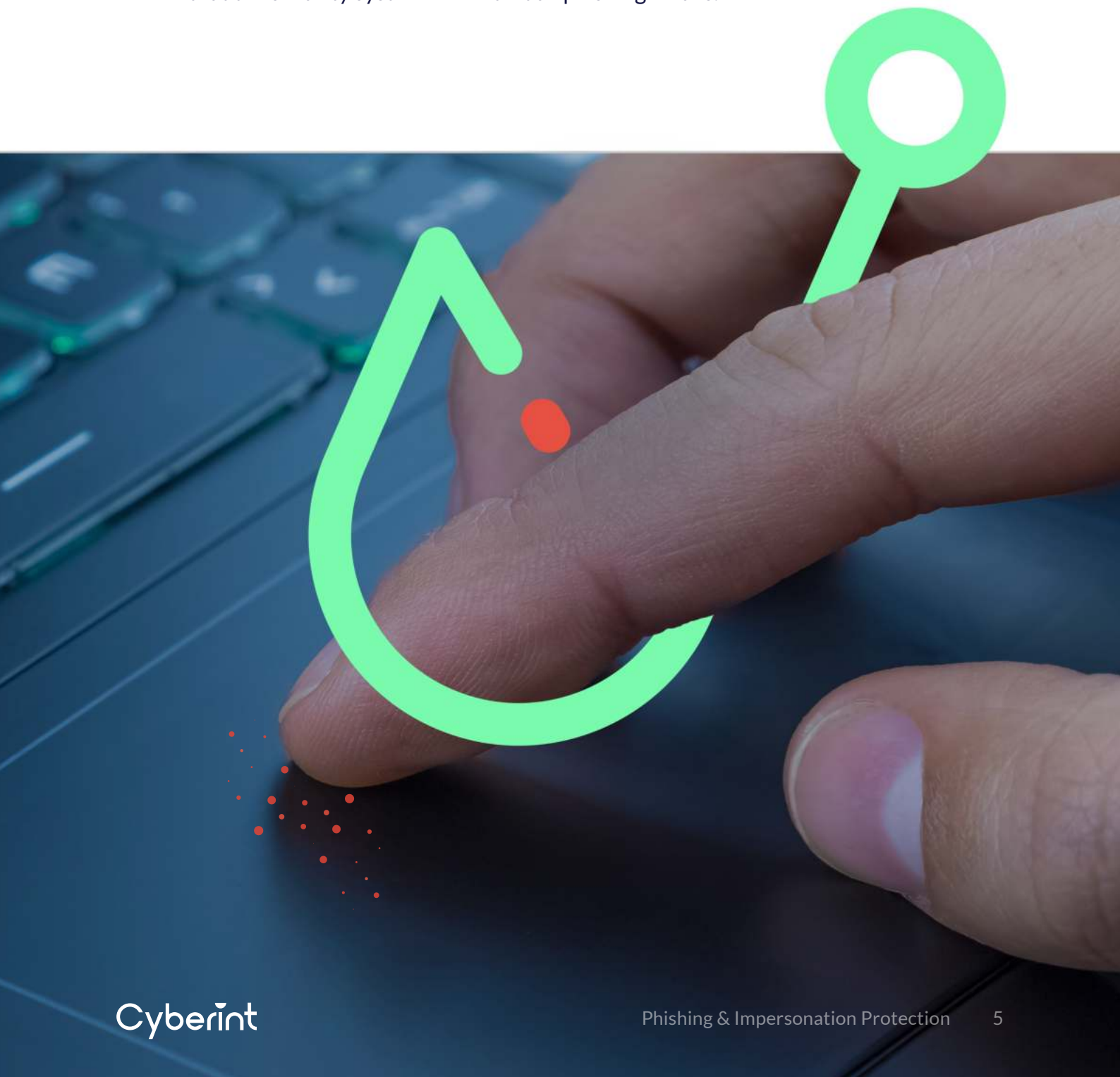
Whatever the goal of a threat actor, every campaign requires setting up a legitimate-looking page, profile or app, to trick the victim into taking the desired action.

In many cases, these campaigns often rely on a combination of elements:

1. A legitimate-looking email, website, app, or profile - as it resembles something the reader would recognize from the past, or includes details that only a legitimate sender would have.

2. Evokes a sense of urgency - in order to lower the defenses of the reader with immediate actions required for immediate gain.

3. No alarms have been set - by the recipient organization security system. As users want to believe that the security system will detect all phishing emails.



Top four types of impersonation attacks

When many people think of phishing, they envision poorly worded emails or text messages that threat actors distribute in an effort to steal sensitive information from their targets.

However, impersonation attacks aren't limited to malicious messages that attackers send en masse to individuals. Imperonation attacks can involve creating entire sites or profiles designed to trick victims into handing over sensitive data.

Three are four main types of impersonation attacks:

Phishing sites:

These are websites designed to mimic a legitimate brand or company. They often ask users to input access credentials they'd use for legitimate sites or upload sensitive personal information.

Social media profiles:

By creating social media profiles that impersonate a legitimate organization, threat actors can engage with unsuspecting targets on social media.

Malicious apps:

In some cases, attackers create entire apps or browser extensions designed to solicit sensitive data.

Executive impersonation:

This type of phishing impersonation happens when threat actors pretend to be an executive or other well- known figure, typically in an effort to trick employees into handing over sensitive information.

Now that we've covered the basics, let's look at each of these types of impersonation in more detail, and discuss what it takes to defend against them.

Phishing Sites

To create phishing sites, threat actors either:

Clone a legitimate website themselves from scratch.

Purchase a phishing kit to help them in this endeavor.

Creating the sites is not particularly challenging, given that threat actors can easily copy logos, fonts and text from legitimate websites. They can even copy the entire source code.

Phishing kits are often available for purchase on deep and dark web forums, making the barrier to enter the phishing industry extremely low.

In addition, to make it harder for victims to distinguish between a phishing site and a "real" site, threat actors often purchase lookalike domains – meaning domains that resemble those of a different company, but are controlled by threat actors (think gogle.com instead of google.com, for example).

They may also compromise existing, legitimate websites and take over their domains.

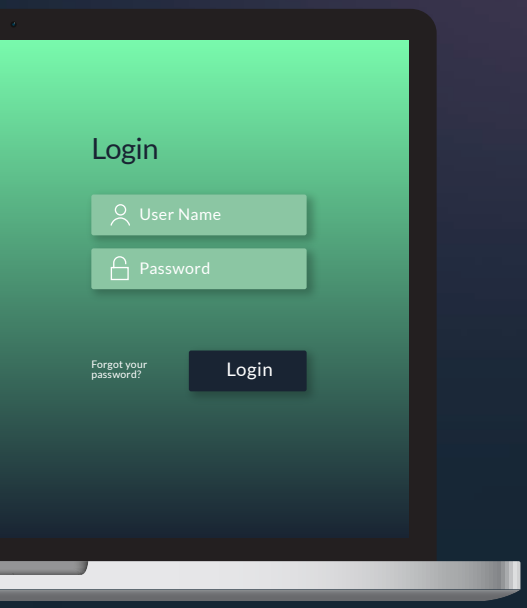
Phishing Delivery

Once the phishing site is ready, the next step in the phishing attack campaign is typically to send phishing emails to potential victims, in order to drive traffic to the malicious site. The threat actor could also choose to distribute the malicious link through other channels such as malvertising, social media etc. To achieve a high rate of response and reduce the chances of having their messages blocked, threat actors often endeavor to distribute messages to a targeted list of users relevant for the phishing campaign.

For instance, rather than blasting emails to a large group of random people that contain links to a phishing site mimicking a bank, threat actors might target only people who they know to be customers of the bank. The ability to purchase email lists – either from legitimate companies that sell data like this for marketing purposes, or by accessing the billions of leaked email addresses available on the Dark Web – helps threat actors curate lists of targets.

Or for example in a malvertising campaign where certain geographies, keywords or users are targeted.

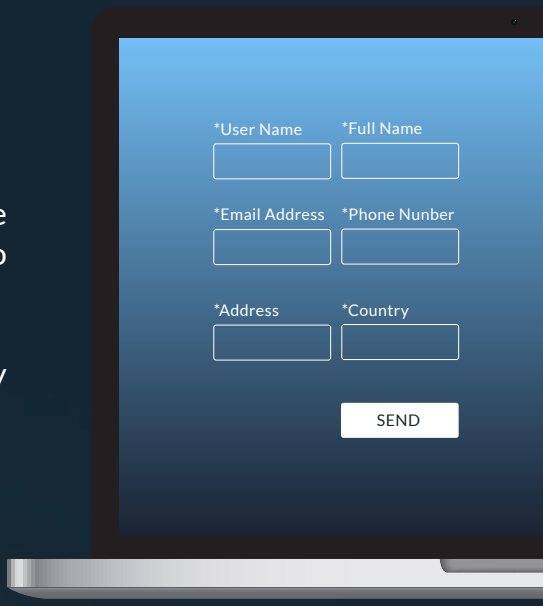
Common Examples of Phishing Sites



A login page for a third-party application that the targeted organization uses, such as Microsoft 365, Salesforce, SAP and so on.

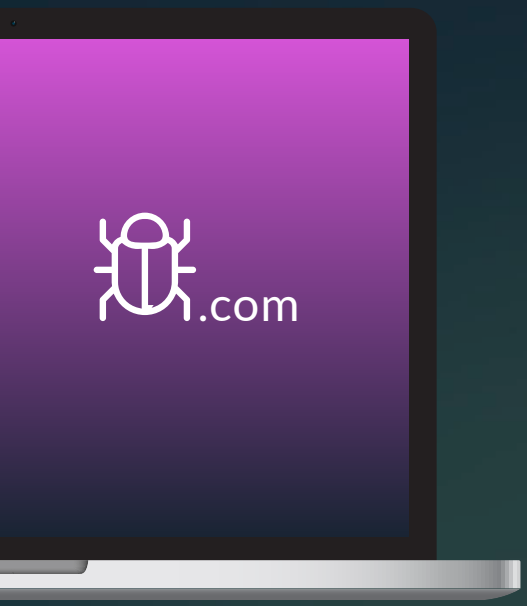
The phishing site will be designed to look exactly like the legit login page of these 3rd party apps If victims enter their access credentials into the site, threat actors can then use the data to log into the company's actual services.

They can also use this method to bypass multi-factor authentication (MFA) because they can ask for the secondary login credential in the same site.



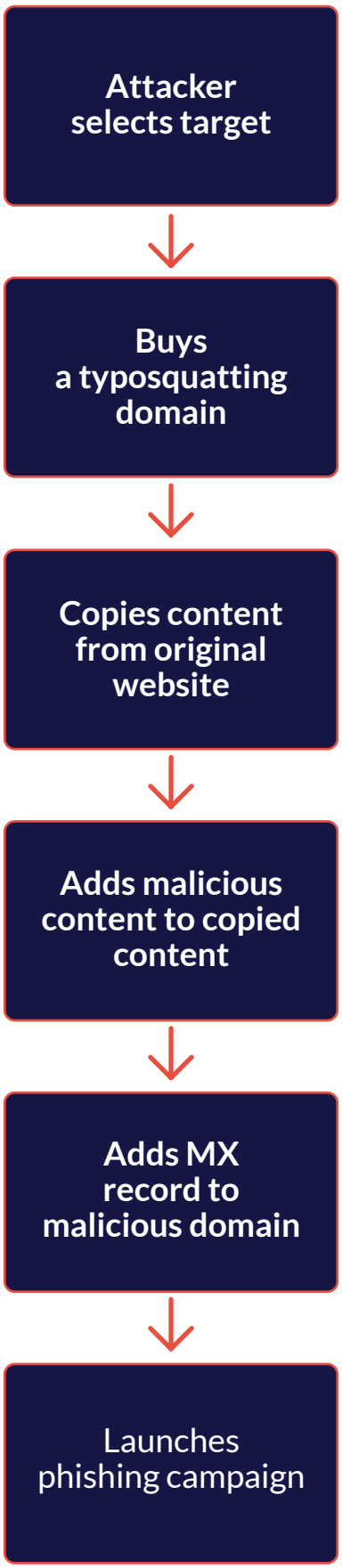
A webpage that requests personal details from users. These are often clones of the legitimate webpage, and their purpose is to trick targets into sharing private information.

If a trusted brand's website is cloned, the user often automatically thinks it's a legitimate and secure site.



A hijacked subdomain that redirects targets to a malicious webpage or installs malware on their devices. If victims look only at the domain inside a link or the one that first loads, without checking the URL again after the redirect, they may not know they're on a phishing site.

The Typical Phishing Attack Timeline



1. Attacker selects a target

2. Attacker purchases a domain

that would be used for the phishing infrastructure. For high efficiency, threat actors usually select a domain which resembles the target organization's main domin, or includes its name. This is done either by creatively searching for a domain permutation or using automated permutation engines to get names and purchase the domain. This is generally referred to as the 'typosquatting domain'.

3. Attacker populates content

that resembles the original website - Text, CSS, logo, and any other element that would help to trick the victims into believing they are on legitimate page. This could be done by their own development or by using a phishing kit available for purchase on the deep and dark web.

4. Attacker adds the malicious content

to the page after creating the apperance of a legitimate page. This could include a credential harvesting tool or a login box in credential collection campaign, or by other means, such as dropping the malicious payload into the victim's machine.

5. Attacker sets up email sending infrastructure

In many cases the domain will be used to send emails from. This technically requires adding a 'mail exchange' (MX) record. The DNS record that will allow email servers to communicate with this email sender and verify that the email delivery will be successful.

6. Attacker launches the campaign

A carefully crafted phishing email using the names and addresses from the obtained email list is then being sent to the entire list.

A Website Takeover Phishing Attack Timeline

1. Attacker selects a target

Either by buying a target or a combo list. A combo list is a text file containing a list of usernames, email addresses and passwords. Those lists are curated by cybercriminals over data breaches or other security incidents then sold or leaked on the dark web so cybercriminals could use them to commit identity theft or other crimes.

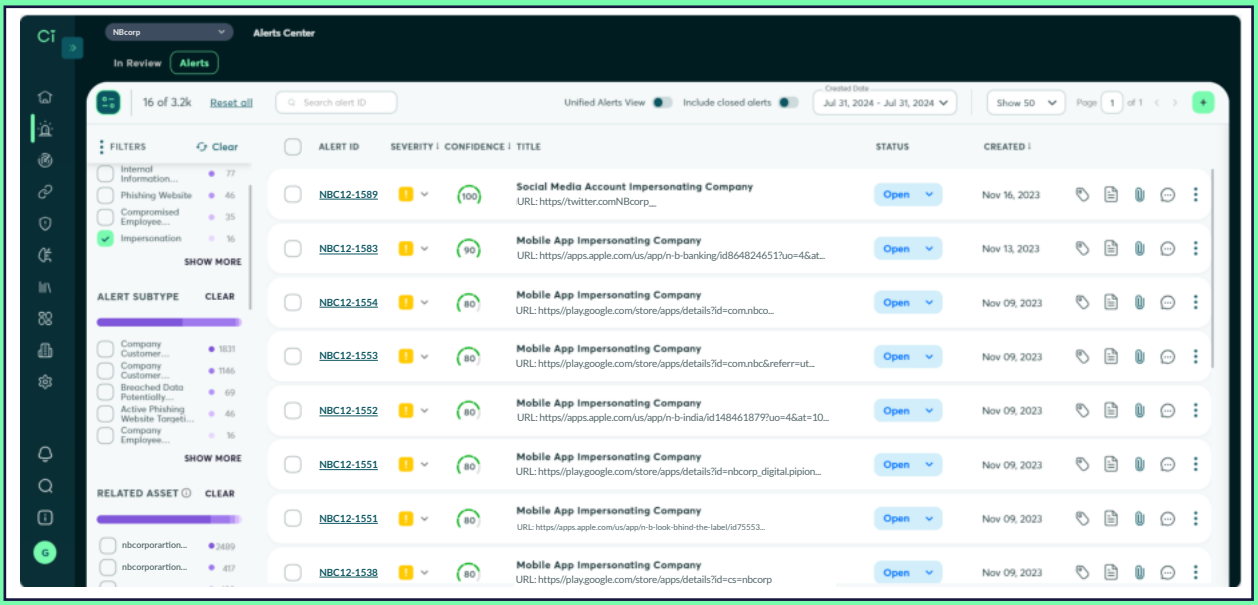
2. Attacker purchases a domain

whether through a phishing exploit kit bought on the deep and dark web or, if they are more advanced, through cross-site scripting (XSS).

3. Attacker launches the campaign

A carefully crafted phishing email using the names and addresses from the list is then being blasted to the entire list.

Impersonation Attacks on Social Media



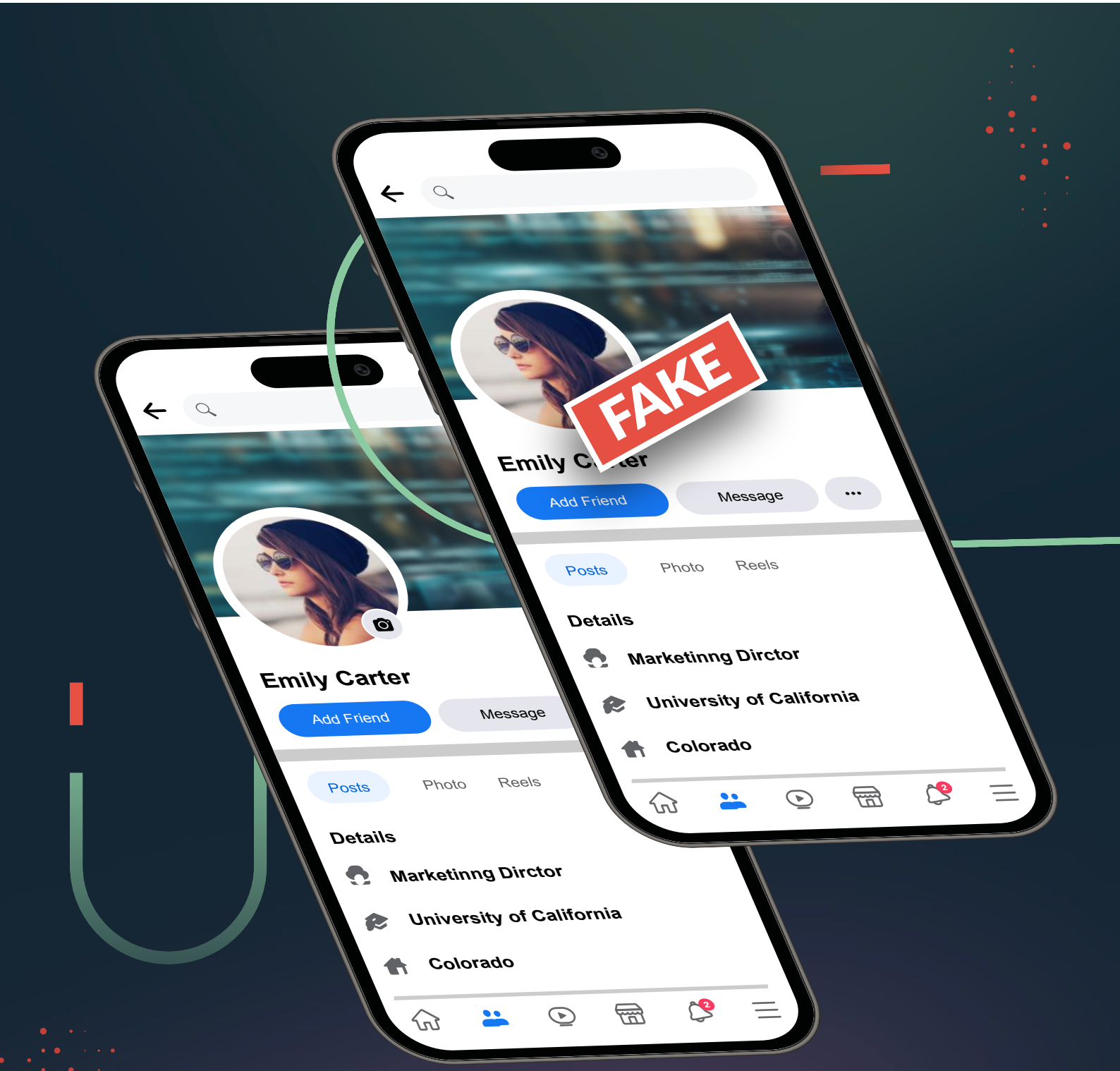
As an alternative to going to the trouble of creating their own phishing websites, threat actors can create fraudulent social media profiles that impersonate brands. By using account names, logos and content similar to those of a legitimate company, threat actors can appear to other social media users as representatives of that company.

Brand impersonation on social media is a relatively easy type of phishing attack to launch because creating social media profiles requires no technical skill, and most social media platforms don't require users to prove they have permission to use certain logos or other content.

Once threat actors create a fraudulent social media account, they can use it to engage directly with a company's customers or followers and solicit sensitive information. They can also launch attacks like malvertising campaigns that distribute content containing links to fraudulent sites.

"The financially motivated threat actor known as FIN7 has been observed leveraging malicious Google ads spoofing legitimate brands as a means to deliver MSIX installers that culminate in the deployment of NetSupport RAT.

"The threat actors used malicious websites to impersonate well-known brands, including AnyDesk, WinSCP, BlackRock, Asana, Concur, The Wall Street Journal, Workable, and Google Meet," cybersecurity firm eSentire said in a report published earlier this week.



Impersonation Attacks via Malicious Apps and Browser Extensions

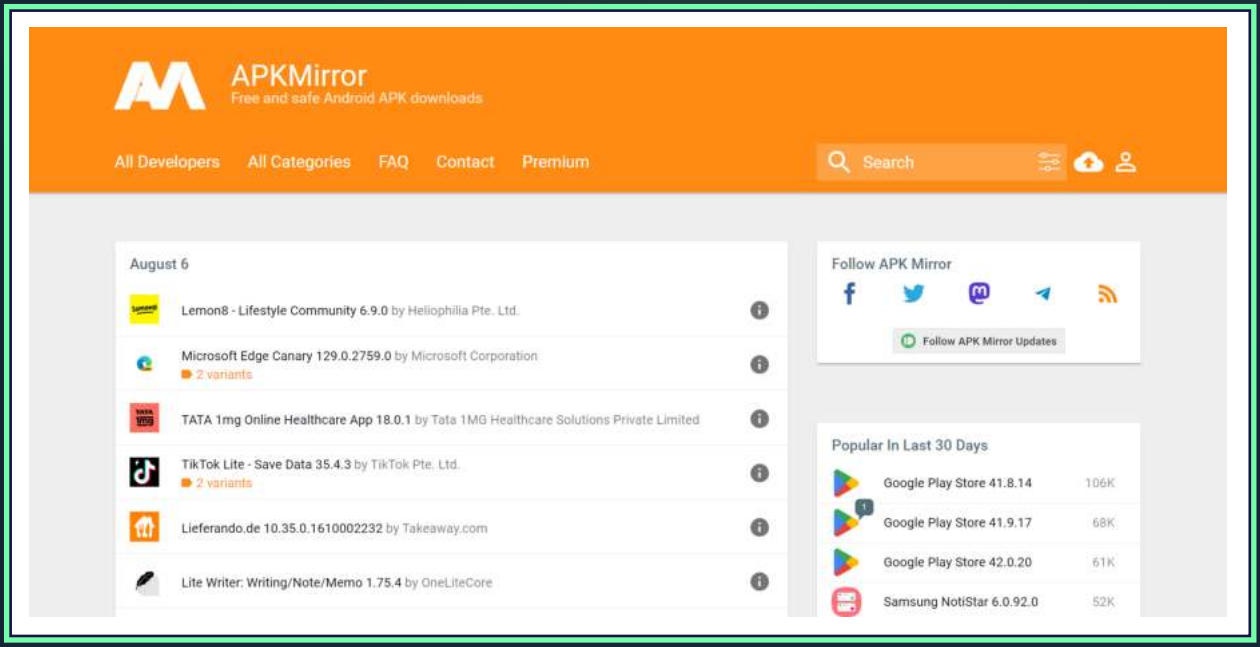
In a world where users are accustomed to downloading applications from app stores with little scrutiny, threat actors can take advantage of this practice by creating malicious apps or browser extensions and distributing them through portals like the Apple App Store and Google Play.

In theory, Google and Apple put guardrails and security checks in place before an individual can make an app available for download. But, of course, these controls sometimes fail and malicious apps end up available despite this.

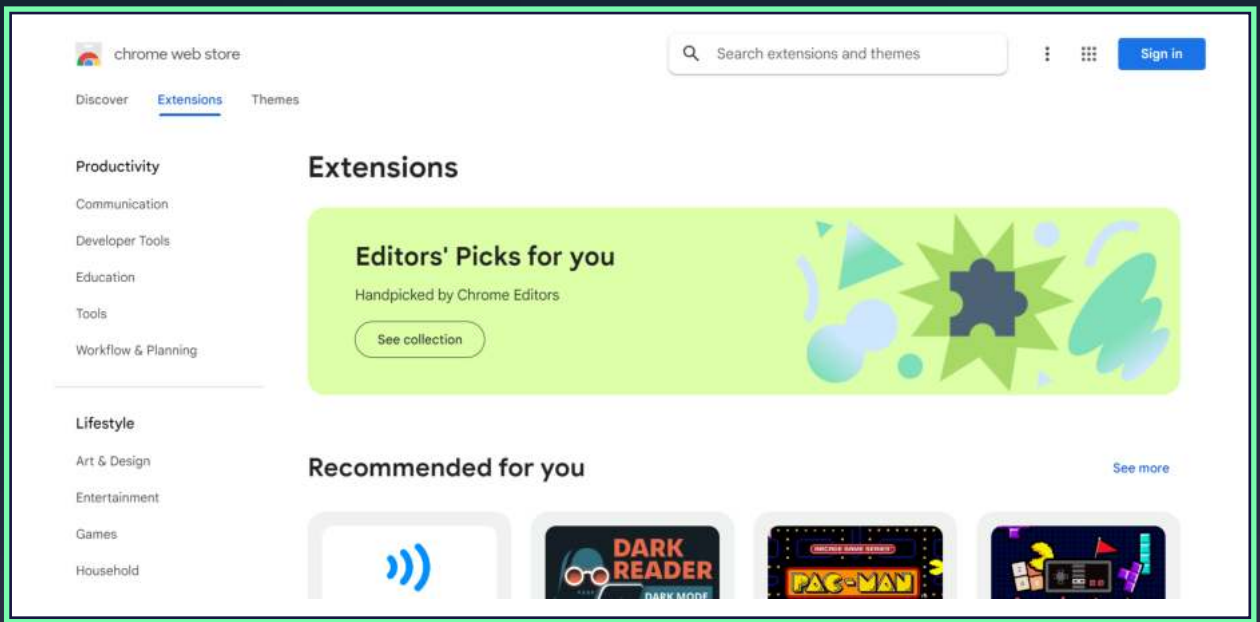
Too often, users assume that they can trust any content in these channels because the app stores themselves are managed by legitimate companies. But the reality is that it's not difficult for threat actors to upload fraudulent apps, and given the large volume of apps, it's impossible for app store maintainers to block them all. Indeed, as of 2021 nearly 2 percent of the top revenue-generating apps in the Apple App Store were scams.

Phishing via Malicious Apps and Browser Extensions

On top of this, threat actors can make use of unofficial app stores - with little to no oversight in terms of brand abuse and security - to distribute malicious software. These app portals are even less monitored and regulated than app stores from Apple and Google, making them unchartered territories.

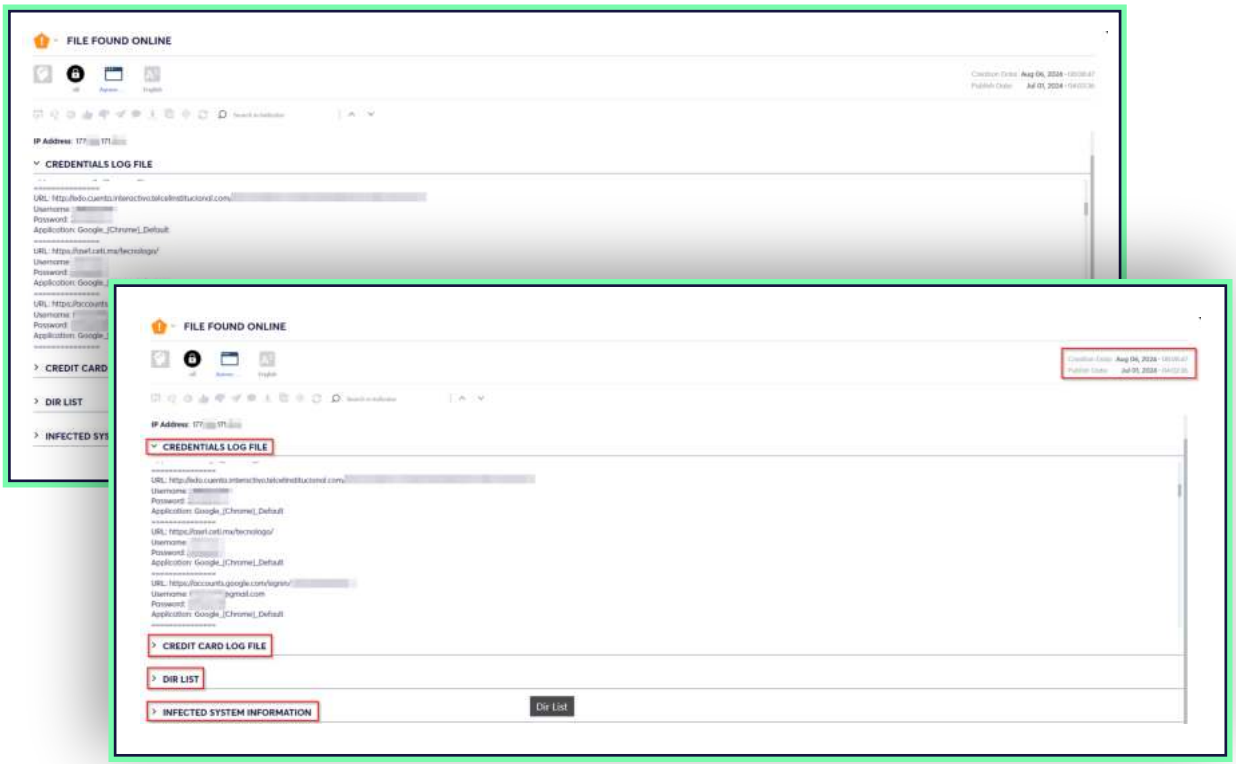


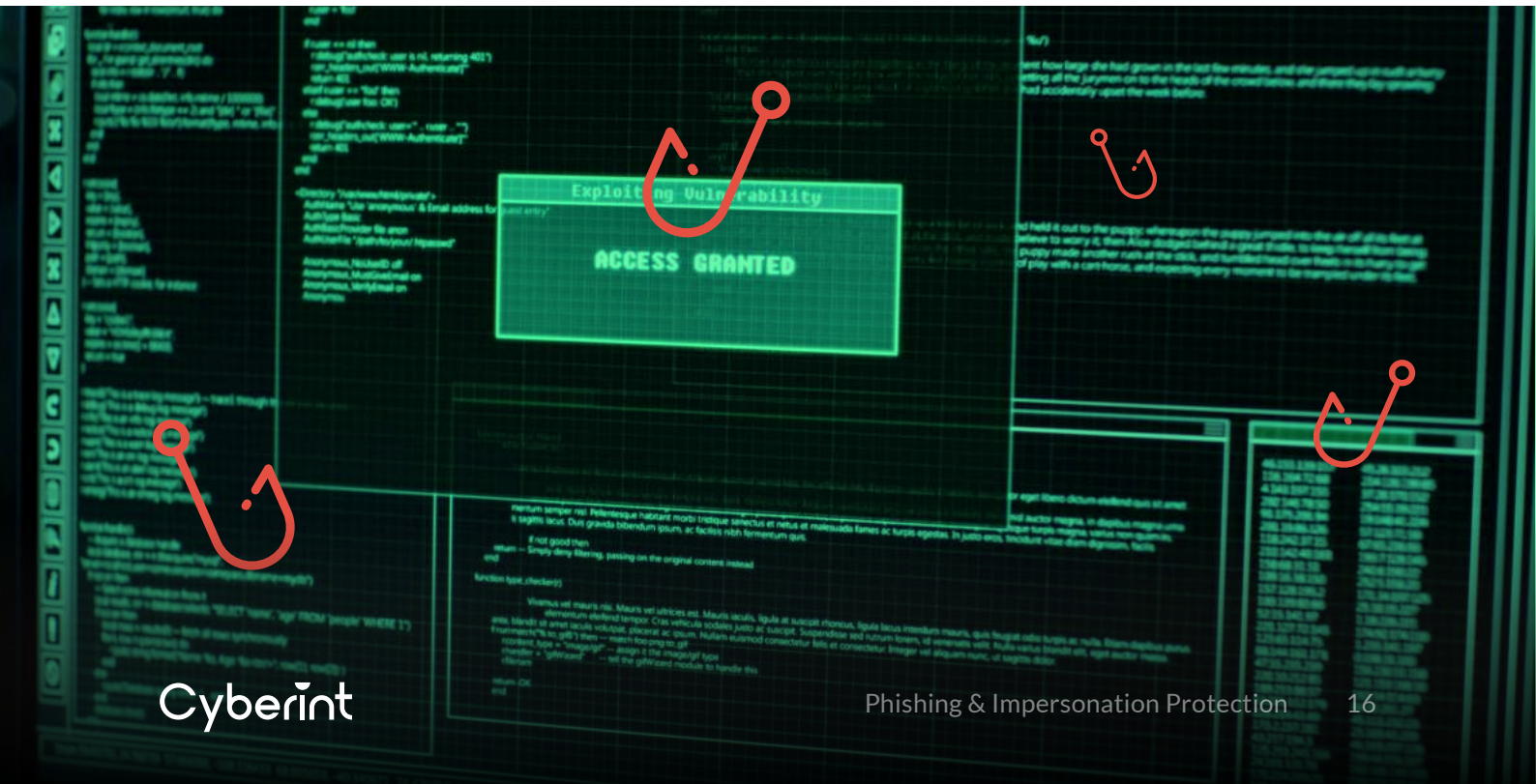
And then there are web browser extensions, which can often be installed directly through browsers or via various websites. This type of software, too, is rarely subject to intensive security validation, making it a prime vehicle for threat actors to plant malicious code on their targets' devices.



Phishing via Malicious apps and Browser Extensions

In short, there are many methods available to threat actors to load fraudulent apps onto victims' computers, phones or tablets. Once installed, the apps can solicit personal information, or, in some cases, exfiltrate it directly from devices as part of an InfoStealer attack.





Executive Impersonation Phishing Attacks

Executive impersonations can happen in multiple ways, such as:

- Fake social media accounts that impersonate an executive at a company.
- An email account with the same name as an executive, or even a spoofed replica of the email address i.e the exact same email@gmail/yahoo/msn etc.
- Phone calls or text messages in which an attacker claims to be an executive.

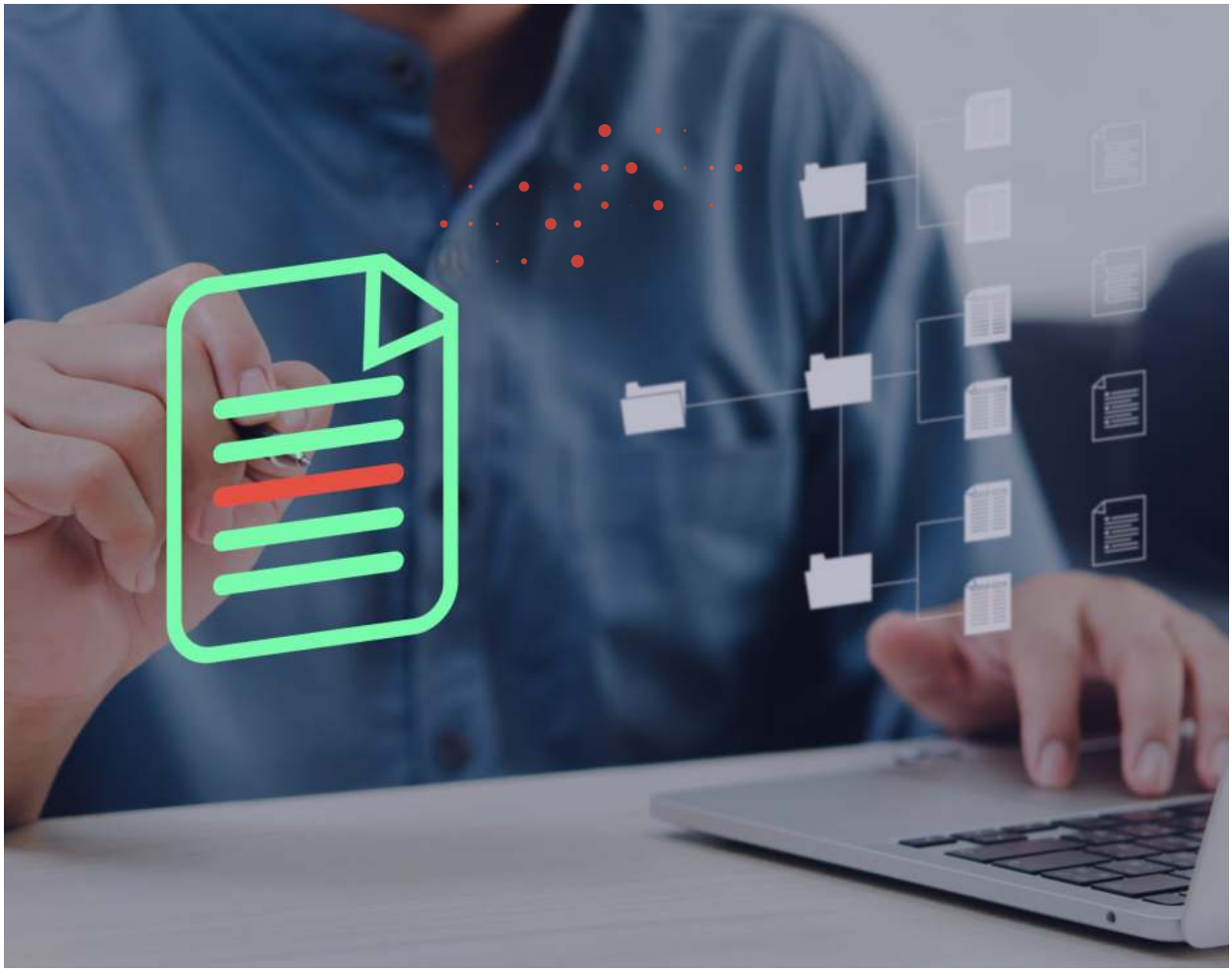
The details of executive impersonation attacks vary, but the underlying technique is the same: Threat actors pretend to be an executive whom their targets recognize.

These attacks often exploit the trust between individuals and high-ranking personnel in organizations, such as CEOs and CFOs. An employee who woul ignore a standard phishing message from an unknown sender might be more hesitant to do so if the employee believes the message came from a company executive.

Threat actors can use executive impersonation attacks to solicit various types of information.

- They might ask employees for login credentials to business systems, for instance.
- Business email compromise is a major concern.
- They might request customer data or financial statements.
- Invoice fraud is a significant concern - Threat actors may update the payment details of an invoice that is due for payment in order to shift the money to an account they control. They might also generate a fake invoice and send it to finance, emphasizing its importance and the need for urgent payment.
- In some cases, executive impersonation can be a means of distributing malware by instructing employees to click nefarious links or install malicious software.

While executive impersonation often targets a company's employees, they're not the only potential victims. Threat actors can also use this type of phishing attack to collect sensitive information from outsiders by, for instance, creating fake job ads, then engaging with applicants while claiming to be legitimate managers or executives of the company.



Phishing Statistics

Number of Phishing Sites per Country

Cyberint analyzed over 5 million phishing sites over the past 60 days to determine how many there are targeting brands in each country. The results are clear the US is highly targeted with 89% of phishing sites targeting brands located in the US.

Most Targeted Countries by Phishing Sites

USA
89%

UK
1.7%

Netherlands
1.7%

Japan
1.2%

Canada
1.2%

Singapore
0.9

France
0.8%

Spain
0.7%

Germany
0.6%

Australia
0.4

Number of Phishing Sites per Industry

Cyberint analyzed over 5 million phishing sites to determine how many phishing websites there are targeting brands in each industry over the past 60 days. Transportation is highly targeted with close to 1/3 of all phishing sites targeting the industry, but the fashion industry is not far behind with 24.5%. Following that is online retail with 16.2%.

Most Targeted Industries by Phishing Sites

Transportation
31.1%

Fashion
24.5%

Online Retail
16.2%

Crypto Exchange
8.1%

Banking
4.7%

Consumer
3.7%

Crypto
2.2%

Telecommunication
1.7%

Social Network
1.4%

Healthcare
1.2%

PHaaS: A new phishing attack threat

Carrying out the types of phishing attacks described above is not trivial. Traditionally, phishing has required threat actors to invest significant time in crafting malicious sites, profiles or apps. They must also sometimes engage at length with their targets. Thus, the "barrier to entry" for launching a phishing attack was somewhat high.

However, Phishing-as-a-Service, or PHaaS, has lowered the bar, making it easier than ever for threat actors to target companies and individuals with various forms of phishing. PHaaS allows threat actors to purchase phishing products or services such as phishing kits. A threat actor with little to no skill can buy a phishing kit and from there it's simple to launch a phishing site (that impersonates a trusted brand out of the box). Phishing kits also set up a C2 server for the threat actor enabling them to receive the data they manage to obtain from victims.

This saves significant time and effort. Instead of having to set up and maintain their own phishing content and infrastructure, they can hire this task out to cybercriminals who specialize in phishing.

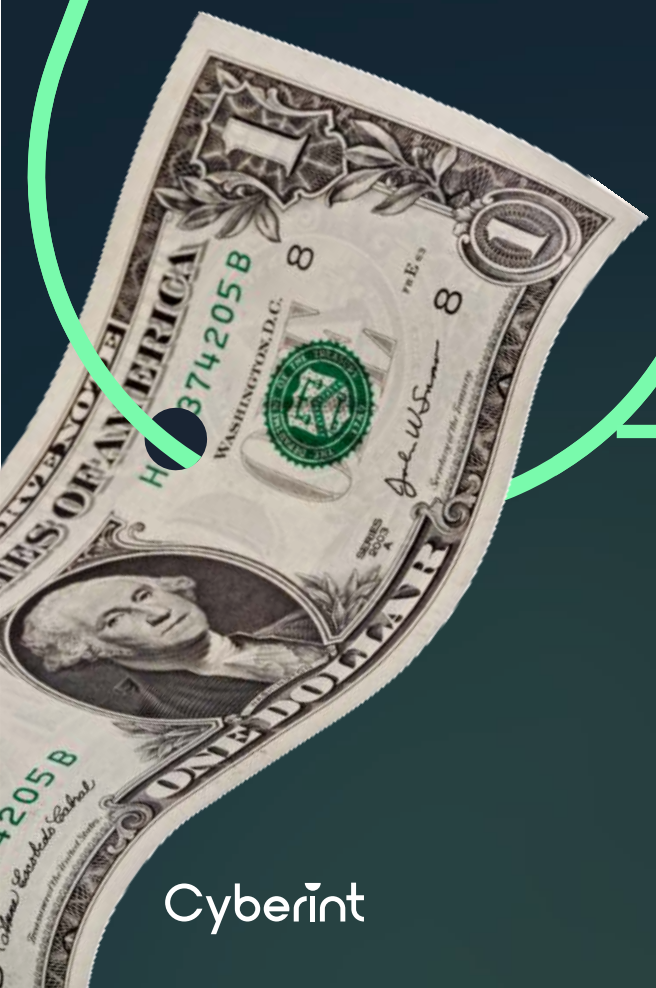
Consequences of Unmitigated Impersonation Attacks

Direct Financial Losses Due To Fraud

Phishing websites that defraud customers or sell counterfeit goods result in a loss of revenue.

Damage To Brand & Consumer Confidence

Victims of scams may place blame on your organization rather than the cybercriminals.



Compliance Challenges & Regulatory Risk

Phishing websites that defraud customers or sell counterfeit goods result in a loss of revenue.

Phishing attack risk mitigation strategies

Faced with such a broad range of attacks, what can companies do to protect themselves from phishing?

A key part of the answer is the concept of defense in depth. Defense in depth means erecting multiple layers of security controls separating your assets from attackers. In the context of phishing in particular, defense in depth is so important because blocking every phishing attack, every time is just not feasible. The high volume of attacks, and the fact that threat actors have so many attack techniques at their disposal, makes it unrealistic to expect to detect phishing attacks involving your company or users before they happen. Plus, the natural inclination of most humans to trust each other means someone will almost always click a malicious link or engage with phishing attackers.

Indeed, as Dark Reading puts it, "The imperfection of humans makes it all but impossible for us to teach everyone how to spot and avoid phishing."

Phishing attack risk mitigation strategies

This is why an effective phishing defense strategy includes a range of protections, such as:

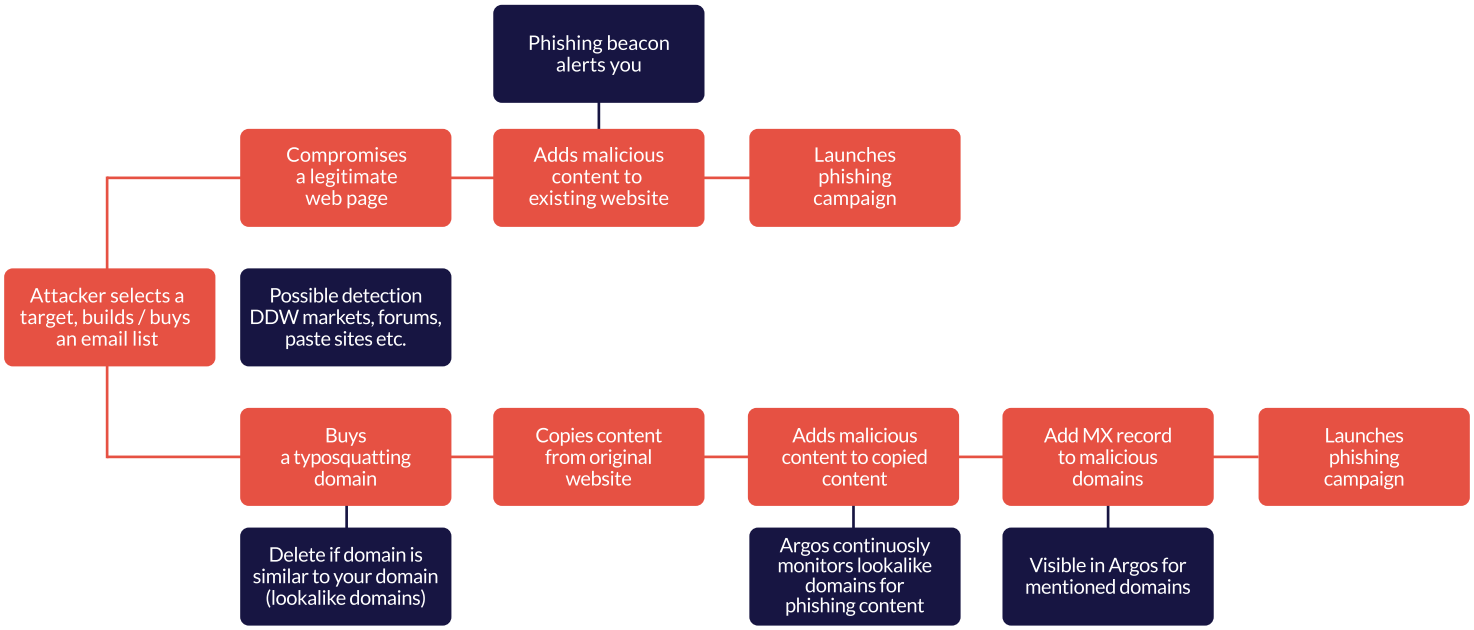
- **Deep and Dark Web monitoring** to detect threat actors who may be planning a phishing attack, to detect phishing kits, or to detect stolen sensitive data that's being sold to alert you to a phishing attack. Cyberint's analysts interact with threat actors to stay on top of new phishing technologies, and Tactics, Techniques, and Procedures (TTPs).

- **Phishing Beacon** so that you can detect if your site is being cloned.

- **Lookalike domain monitoring** so you can detect if a phishing attack is being planned and monitor it closely. Cyberint continuously monitors for similarities between your domains and the newly registered candidates to provide a level of indication of malicious intent, and alerts you of suspicious, newly registered lookalike domains.

- **Social media monitoring** to alert you to brand impersonation attacks and executive impersonation attacks on social media

- **App Store Monitoring** to alert you of impersonations on both official and unofficial mobile app stores, as well browser extension platforms.



Cyberint also detects hijackable subdomains

You Can't Avoid Phishing,

But You Can Mitigate the Risk

Phishing isn't going away. On the contrary, it's likely to become an even more pervasive threat in the coming years due to innovations like AI and the availability of PHaaS. But that doesn't mean companies have to give up and accept pervasive phishing risks as a fact of life. With effective security controls that enable a defense in depth, minimizing the riskof successful phishing attacks is well within reach.

Speak to a Phishing Expert

Contact Us

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

ISRAEL

Tel: +972 3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House
14-18 Great Titchfield Street,
London, W1W 8BD

USA – TX

Tel: +1-646-568-7813
7250 Dallas Pkwy STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform's patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://Cyberint.com.