

The State of Security (<https://www.tripwire.com/state-of-security/>)

NEWS. TRENDS. INSIGHTS.

6 Common Phishing Attacks and How to Protect Against Them



DAVID BISSON ([HTTPS://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/DAVID-BISSON/](https://www.tripwire.com/state-of-security/contributors/david-bisson/))

([HTTPS://V](https://v) Follow @DMBisson ↘)

/STATE- OCT 7, 2019 |

OF- SECURITY AWARENESS (/STATE-OF-SECURITY/TOPICS/SECURITY-AWARENESS/)

SECURITY

/CONTRIBUTORS

/DAVID-


BISSON/)




(https://www.tripwire.com/solutions/configure-and-harden-your-systems/security-configuration-management-for-dummies-book-register/?utm_source=sos&utm_medium=sbnr&utm_content=pdf&utm_campaign=scm-for-dummies)




(<https://devops.tripwire.com/register?referredby=socialmedia/?blog>)

 ([http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/security-](http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/)


[awareness/6-common-phishing-attacks-and-how-to-protect-against-them/](http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/))  ([http://twitter.com/intent](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&via=tripwireinc)

[/tweet?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6 Common Phishing Attacks and How to Protect Against](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&via=tripwireinc)

[Them&via=tripwireinc](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&via=tripwireinc))  ([http://www.linkedin.com/shareArticle?mini=true&url=https:](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them)

[//www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6 Common Phishing Attacks and How to Protect Against Them](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them)) 

([http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security/security-awareness/6-](http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/)

[common-phishing-attacks-and-how-to-protect-against-them/](http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/))  ([mailto:?subject=6 Common Phishing](mailto:?subject=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&body=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/)

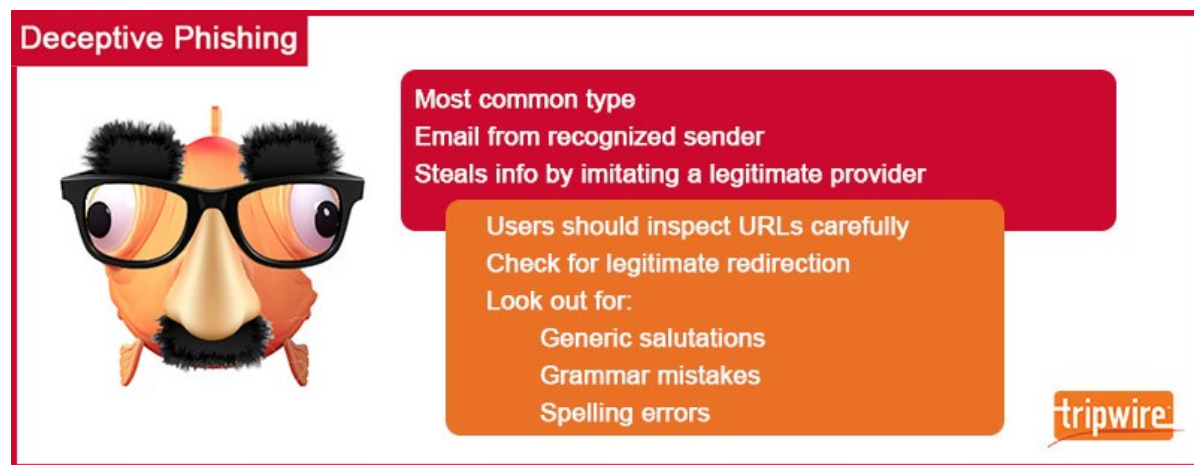
[Attacks and How to Protect Against Them&body=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/](mailto:?subject=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&body=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/))

Phishing attacks don't show any sign of slowing down. Per its 2019 Phishing Trends and Intelligence Report, PhishLabs (<https://info.phishlabs.com/hubfs/2019%20PTI%20Report>

([/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf](#)) found that total phishing volume rose 40.9 percent over the course of 2018. These attacks targeted a range of organizations, especially financial service companies, email and online service providers and cloud (<https://www.tripwire.com/solutions/maintain-control-in-the-cloud/>)/file hosting firms. It's, therefore, no surprise that Verizon's 2019 Data Breach Investigations Report (<https://enterprise.verizon.com/resources/reports/dbir/>) (DBIR) found phishing to be the top threat action variety in all breaches analyzed during the reporting period.

The growth of phishing attacks poses a significant threat to all organizations. It's important that all companies know how to spot some of the most common phishing scams if they are to protect their corporate information. Towards that end, we at *The State of Security* will discuss six of the most common types of phishing attacks below as well as provide useful tips on how organizations can defend themselves.

1. DECEPTIVE PHISHING



(<https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Deceptive-Fact-File-v3.jpg>)

Deceptive phishing is by far the most common type of phishing scam. In this type of ploy, fraudsters impersonate a legitimate company in an attempt to steal people's personal data or login credentials. Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

As an example, PayPal scammers (<https://www.paypal.com/us/brc/article/what-is-phishing-or-spoofing>) could send out an attack email that instructs recipients to click on a link in order to rectify a discrepancy with their account. In actuality, the link redirects to a fake PayPal login page that collects a victim's login credentials and sends them to the attackers.

The success of a deceptive phish hinges on how closely the attack email resembles a piece of official correspondence from the abused company. As a result, users should inspect all URLs carefully to see if they redirect to an unknown and/or suspicious website. They should also look out for generic salutations, grammar mistakes and spelling errors scattered throughout the email.

2. SPEAR PHISHING



(<https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Spear-Factfile.jpg>)

Not all phishing scams embrace “spray and pray” techniques at the expense of personalization. Some ruses rely on a personal touch quite heavily. They wouldn't be successful otherwise.

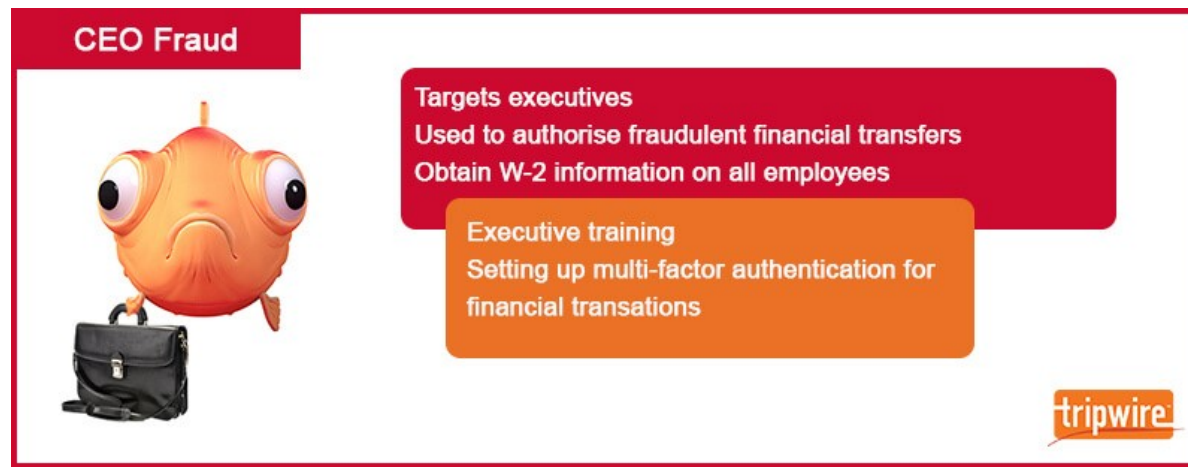
Enter spear phishing schemes.

In this type of play, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the

recipient into believing that they have a connection with the sender. The goal is the same as deceptive phishing, even so: trick the victim into clicking on a malicious URL or email attachment so that they will hand over their personal data. Given the amount of information needed to craft a convincing attack attempt, it's no surprise that spear-phishing is commonplace on social media sites like LinkedIn (<https://www.tripwire.com/state-of-security/security-awareness/a-guide-on-5-common-linkedin-scams/>) where attackers can use multiple data sources to craft a targeted attack email.

To protect against this type of scam, organizations should conduct ongoing employee security awareness training that, among other things, discourages users from publishing sensitive personal or corporate information on social media. Companies should also invest in solutions that analyze inbound emails for known malicious links/email attachments. This solution (<https://www.tripwire.com/solutions/tripwire-malware-detection/>) should be capable of picking up on indicators for both known malware and zero-day threats.

3. CEO FRAUD



(<https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/CEO-Factfile.jpg>)

Spear phishers can target anyone in an organization, even executives. That's the logic behind a "whaling (<https://www.tripwire.com/state-of-security/security-awareness/whaling-attacks-tracing-the-evolution-of-phishing-attacks/>)" attack. In these scams,

fraudsters try to harpoon an exec and steal their login details.

In the event their attack proves successful, fraudsters can choose to conduct CEO fraud. As the second phase of a business email compromise (<https://www.tripwire.com/state-of-security/latest-security-news/business-email-compromise-scam-alert-issued-by-fs-isac/>) (BEC) scam, CEO fraud is when attackers abuse the compromised email account of a CEO or other high-ranking executive to authorize fraudulent wire transfers to a financial institution of their choice. Alternatively, they can leverage that same email account to conduct W-2 phishing in which they request W-2 information for all employees so that they can file fake tax returns on their behalf or post that data on the dark web.

Whaling attacks work because executives often don't participate in security awareness training with their employees. To counter the threats of CEO fraud and W-2 phishing, organizations should mandate that all company personnel—including executives—participate in security awareness training on an ongoing basis.

Organizations should also consider injecting multi-factor authentication (MFA) channels into their financial authorization processes so that no one can authorize payments via email alone.

4. VISHING



(<https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Vishing-Factfile.jpg>)

Until now, we've discussed phishing attacks that rely solely on email as a means of communication. Email is undoubtedly a popular tool among phishers. Even so, fraudsters do sometimes turn to other media to perpetrate their attacks.

Take vishing, for example. This type of phishing attack dispenses with sending out an email and instead goes for placing a phone call. As noted by Comparitech (<https://www.comparitech.com/blog/information-security/common-phishing-scams-how-to-avoid/>), an attacker can perpetrate this type of attack by setting up a Voice over Internet Protocol (VoIP) server to mimic various entities in order to steal sensitive data and/or funds.

These vishing attacks have taken on various forms. In September 2019, for instance, Infosecurity Magazine (<https://www.infosecurity-magazine.com/news/mps-bombarded-spam-brexit-no-deal/>) reported that digital attackers launched a vishing campaign to try to steal the passwords of UK MPs and parliamentary staffers. Not long thereafter, The Next Web (<https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/>) covered an attack where vishers masqueraded as the boss of a German parent company to scam a UK subsidiary firm out of \$243,000.

To protect against vishing attacks, users should avoid answering calls from unknown phone numbers, never give out personal information over the phone and use a caller ID app.

5. SMISHING



(<https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Smishing-Factfile.jpg>)

Vishing isn't the only type of phishing that digital fraudsters can perpetrate on a phone. They can also conduct what's known as smishing. This method leverages malicious text messages to trick users into clicking on a malicious link or handing over personal information.

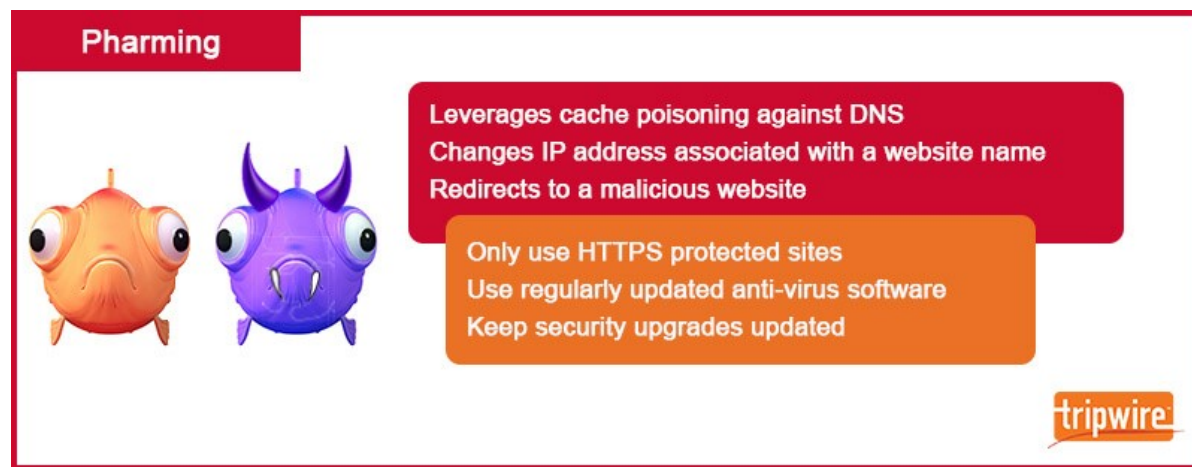
Like vishers, smishers pose as various entities to get what they want. Back in February 2019, for instance, Nokia warned its users to be on the lookout for a smishing campaign in which digital attackers posed as the Finnish multinational telecommunications and sent out text messages informing users that they had won a car or money. The bad actors then asked recipients to send over money as a registration payment for their new car, reported Bleeping Computer (<https://www.bleepingcomputer.com/news/security/lucky-draw-smishing-campaign-asks-money-to-deliver-car-prize/>).

Later in the year, WATE (<https://www.wate.com/investigations/knoxville-woman-taken-in-by-text-message-smishing-scam/>) covered the story of a Knoxville woman who fell for a smishing attack. The woman had cancer, and the scammers claimed that she could receive a federal grant to assist her in paying for treatment. She just needed to submit a down payment and pay taxes on the grant first, the fraudsters told her.

Users can help defend against smishing attacks by researching unknown phone numbers thoroughly and by calling the company named in the messages if they have

any doubts.

6. PHARMING



(<https://3b6xlt3iddqmuq5vy2w0s5d3-wpengine.netdna-ssl.com/state-of-security/wp-content/uploads/sites/3/Pharming-Factfile.jpg>)

As users become wiser to traditional phishing scams, some fraudsters are abandoning the idea of “baiting” their victims entirely. Instead, they are resorting to pharming (<http://us.norton.com/cybercrime-pharming>). This method of phishing leverages cache poisoning against the domain name system (DNS), a naming system that the Internet uses to convert alphabetical website names, such as “www.microsoft.com,” to numerical IP addresses so that it can locate and thereby direct visitors to computer services and devices.

Under a DNS cache poisoning attack, a pharmer targets a DNS server and changes the IP address associated with an alphabetical website name. That means an attacker can redirect users to a malicious website of their choice. That’s the case even if the victim enters the correct site name.

To protect against pharming attacks, organizations should encourage employees to enter in login credentials only on HTTPS-protected sites. Companies should also implement anti-virus software on all corporate devices and implement virus database updates on a regular basis. Finally, they should make sure to stay on top of security upgrades issued by a trusted Internet Service Provider (ISP).

CONCLUSION

Using the guide above, organizations will be able to more quickly spot some of the most common types of phishing attacks. Even so, that doesn't mean they will be able to spot each and every phish. Phishing is constantly evolving to adopt new forms and techniques.

With that in mind, it's imperative that organizations conduct security awareness training on an ongoing basis so that their employees and executives can stay on top of phishing's evolution.

For more information on how your company's personnel can spot a phish, please click here (<https://www.tripwire.com/state-of-security/security-awareness/avoiding-the-bait-helpful-tips-to-protect-yourself-against-phishing-scams/>).

SHARE THIS POST



(<http://www.facebook.com/sharer.php?u=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/>)



([http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6 Common Phishing Attacks and How to Protect Against Them&via=tripwireinc](http://twitter.com/intent/tweet?url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&via=tripwireinc))

[http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6 Common Phishing Attacks and How to Protect Against Them](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them)



([http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6 Common Phishing Attacks and How to Protect Against Them](http://www.linkedin.com/shareArticle?mini=true&url=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/&text=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them))




(<http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security>

<http://www.reddit.com/submit?url=https://www.tripwire.com/state-of-security>

[mailto:?subject=6 Common Phishing Attacks and How to Protect Against Them&body=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/](mailto:?subject=6%20Common%20Phishing%20Attacks%20and%20How%20to%20Protect%20Against%20Them&body=https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/))



(mailto:?)



tripwire

The Executive's Guide to the CIS Controls

Key Takeaways & Action Opportunities

[Download Now](#)

(<https://www.tripwire.com/misc/executives-guide-top-20-critical-security-controls-register/?referredby=blogbottom/>)

TOPICS

- [ICS Security \(/state-of-security/topi...\)](#)
- [Cloud \(/state-of-security/topics/sec...\)](#)
- [IT Security and Data Protection \(/st...\)](#)
- [Latest Security News \(/state-of-sec...\)](#)
- [Regulatory Compliance \(/state-of-s...\)](#)
- [Government \(/state-of-security/topi...\)](#)
- [Vulnerability Management \(/state-o...\)](#)

ABOUT

- [About \(/state-of-security/about/\)](#)
- [Contributors \(/state-of-security /contributors/\)](#)
- [Write for us \(/state-of-security/about /contact-us/\)](#)
- [Privacy Policy \(/legal/privacy/\)](#)
- [Tripwire.com \(/\)](#)

CONTACT US

US Headquarters
 308 SW 2nd Ave Suite 400
 Portland, OR 97204
 (<https://www.google.com/maps/place/Tripwire/@45.5201564,-122.673347,19z/data=!3m1!4b1!4m5!3m4!1s0x54950a0fb0c4e8f1:0x5e346d3964f079a2!8m2!3d45.5201564!3d-122.6727998>)

Direct: 503.276.7500
 (tel:5032767500)

SEARCH

[International Offices \(/contact/\)](/contact/)

© 2019 Tripwire, Inc. ([//tripwire.com/](https://tripwire.com/)) All rights reserved.