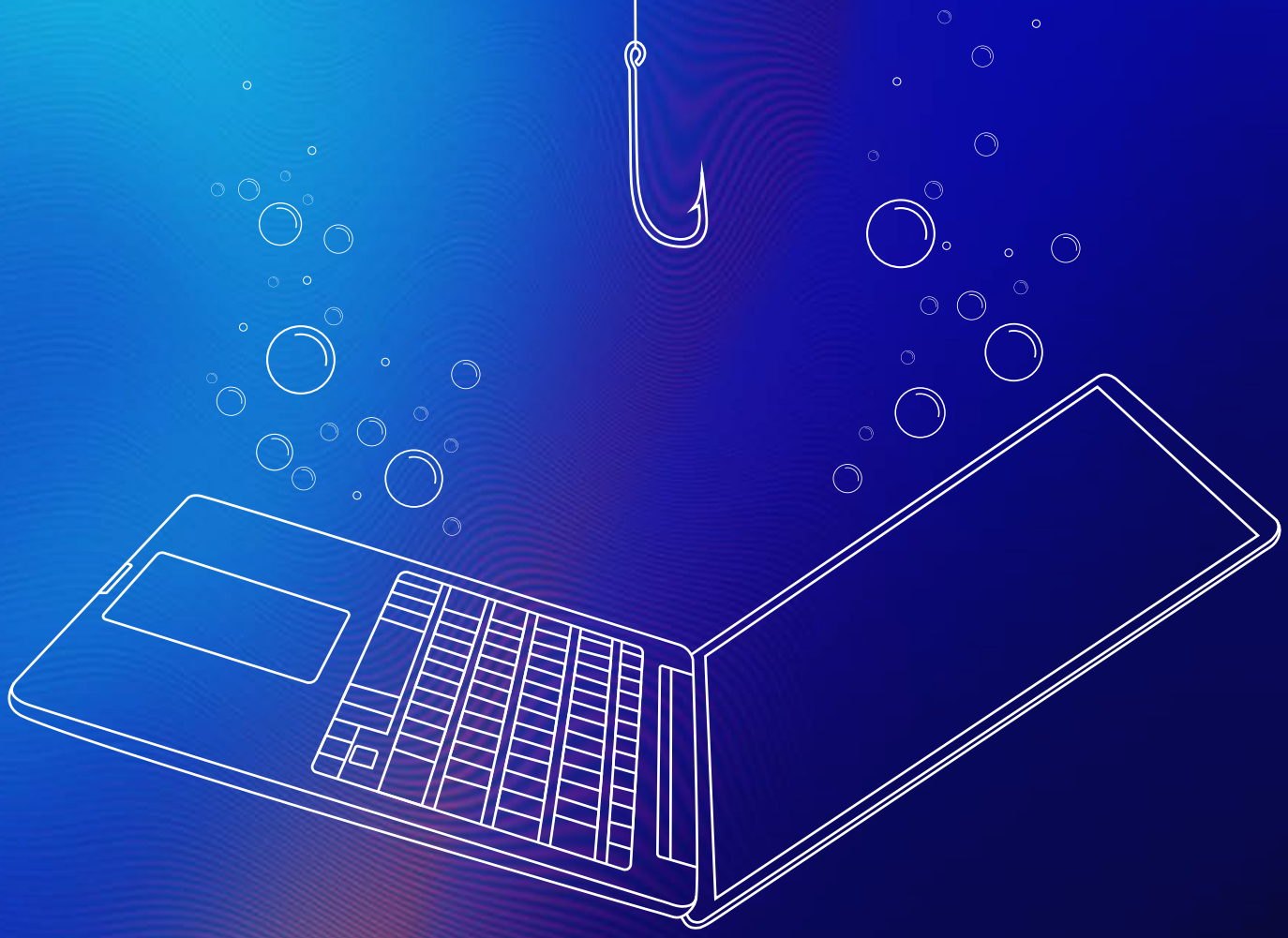
HYPR

PHIGHT BACK AGAINST PHISHING

Best Practices to Protect Your Organization



Introduction

Nobody needs to be convinced that phishing attacks are a large and growing problem for every enterprise. The only question is how bad it will get. According to the Verizon Data Breach Investigations Report, phishing accounted for 36% of data breaches in 2021 — up from 25% in 2020.[1]

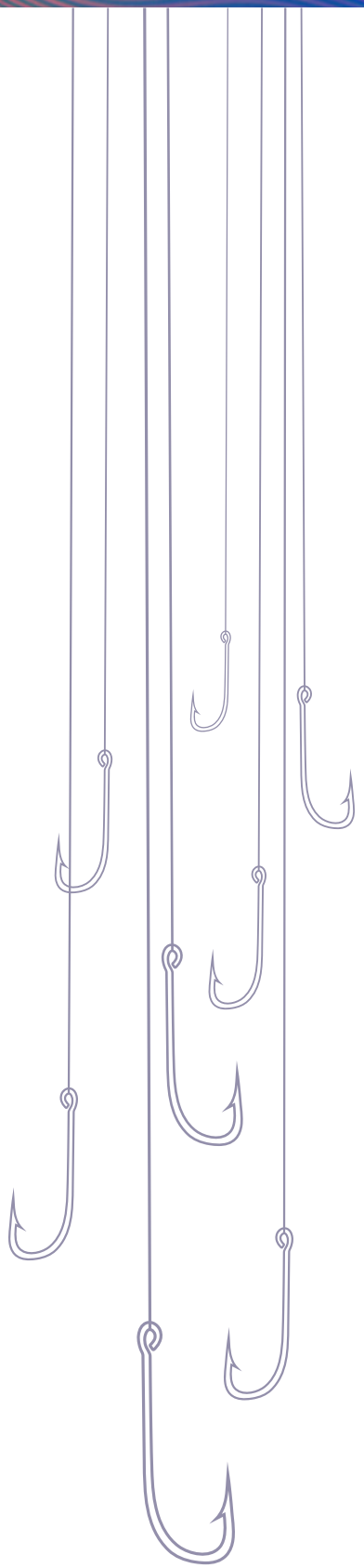
Breaches aren't the only phishing threat. Phishing is the initial vector in attacks to steal credentials, initiate fraudulent transactions, deliver malware such as infostealers or ransomware, and to gain a foothold to move laterally through a system. For example, Twitter made headlines for all the wrong reasons when a 2020 spear phishing attack allowed hackers to tweet a bitcoin scam from high-profile accounts, including Barack Obama and Bill Gates.[2]

Phishing Harms Organizations of All Sizes

But if you think hackers only go after big companies, think again. A recent analysis by Analyst1, a threat intelligence firm, indicates that in 2022, criminal networks will increasingly shift their attacks from high-profile targets to smaller companies in order to evade "unwanted attention from the federal government."[3] Small- to medium-size businesses are also more attractive targets because they typically have fewer security measures in place.

The damage from a single, successful phishing attack can be severe and lasting. Phishing costs organizations an annual average of nearly $15 million, with expenses ranging from ransom demands to malware clean-up to lost productivity.[4] Credential compromises account for the largest percentage of costs, including containing the attack when possible and mitigating damage when not. Beyond these direct costs, an organization may lose customers, face higher insurance premiums, and see its reputation suffer.

Phishing is clearly a problem you can't ignore. But there's good news. As this guide shows, there are common-sense steps you can take today to keep phishing attacks from crippling your business.



THERE'S MORE THAN ONE WAY TO PHISH

The first step of the anti-phishing fight is to know your enemy. Phishing comes in several varieties, and it's important to understand the most common types so you can guard against them. They include:

Mass Email Phishing

This type of attack targets the unaware with bulk emails, usually with a link to a fraudulent site that appears legitimate. Victims are then prompted to input information, such as their username and password, thereby enabling other attacks. Cybercriminals can purchase phishing kits and email lists on the dark web fairly cheaply. They target users of all sizes and types, hoping to trick them into a response they can leverage.

Spear Phishing and Whaling

As the names suggest, these types of phishing are more targeted and go after higher-value victims ("whales" such as CEOs or other prominent individuals). Attackers send targeted emails to specific people within an organization, trying to gain access to an employee or executive's system. These attacks are more personalized, purportedly coming from trusted suppliers or colleagues. Once they have taken over a corporate account, hackers often attempt to initiate a fraudulent financial transaction. For example, an attacker posing as a CEO might request gift cards to be issued to employees with the card numbers sent back to them for "tracking." Spear phishing is much more likely to succeed than other methods. Symantec's Internet Security Threat Report names spear phishing, at 65%, as the most common infection vector in a targeted attack.[5]

SMS Phishing ("Smishing")

In this type, text messages replace email as the phishing medium, but the mode of attack is otherwise the same. Users receive a text message supposedly from a trusted business, such as their bank or a government department. The text typically directs them to respond to an "urgent" situation by following a link and logging in using their password. Smishing has become increasingly common. The British government's Revenue and Customs department reported that SMS phishing attempts increased 700% in the first half of 2021.[6]

SMS PHISHING ATTEMPTS INCREASED 700% IN THE FIRST HALF OF 2021.

All types of phishing work by prompting the user to take an action — either clicking a link and entering exploitable information or clicking an email attachment that deploys malware, including ransomware, that can then spread throughout an organization's systems. Therefore, any successful anti-phishing strategy should focus on measures that prevent users from taking those actions.

THE BARE MINIMUM

If your organization is just beginning its anti-phishing efforts, these simple practices offer some limited defense.

Domain Checking

Attackers can spoof the name that appears as an email's "sender" or could be using a previously compromised account to elevate their attack. They often use tricks such as deceptive spelling. Remind users to hover over the sending address or link to check that it aligns with what's expected.

Password Hygiene

Passwords are often the only form of protection for accounts and systems, making them a major focus for attackers. What's more, people frequently reuse the same passwords across many services. That means a single breach could lead to all of their accounts being compromised. If your organization still uses passwords, at least maintain password hygiene — require that users replace passwords at regular intervals, never reuse the same password for different accounts, and use long, complex passwords or passphrases.

Social Media Awareness

Most people freely provide personal information on social media, which a bad actor can use in targeted spear phishing attacks. Instruct users to be wary of "fun" quizzes or people they meet online or through apps that ask for unnecessary information. Attackers are skilled at extracting data — such as birthdays or first pets — which can then be used in credential stuffing attacks to answer follow-up security questions.

The problem with all of these measures is that they require education and a commitment from all users to work. You may train everyone to follow these steps — and issue frequent reminders — but all it takes is one lapse by one person to foil your best efforts. Do you really want to put your users in charge of your anti-phishing program? And if your organization's email server has been breached or a trusted person's account taken over, even scrupulous vigilance isn't enough.

USEFUL, BUT STILL LIMITED

Even people who are committed to combating phishing will occasionally err — and as hackers become more sophisticated, their efforts are increasingly effective and difficult to spot. The following defensive measures are useful, but not ironclad.

Adopt Multi-Factor Authentication

Multi-factor authentication (MFA) requires people to use additional methods to prove their identity when they log into a system or launch an application. It means that even if attackers succeed in getting a username and password, they will still need the additional factor. The most common MFA types are one-time SMS codes, push notifications, and software tokens. These add a layer of security but, unfortunately, are still vulnerable as noted in a recent analysis issued by the U.S. Cybersecurity & Infrastructure Security Agency (CISA).[7] Criminals have already developed attacks that can circumvent traditional MFA systems, aided by widely available tools like Modlishka and Snipr.

MFA solutions that do not use a one-time password (OTP) or other phishable factor bring greater security. **Beware, however, of deploying solutions that make the login process too cumbersome, as your users may resist adoption or find workarounds.**

Train, Test and Repeat

Teams at all levels should be trained on sound phishing prevention tactics, such as never forwarding suspicious emails to others (except to report them to your security team) or opening an attachment they do not expect. Anti-phishing training has been proven to reduce phishing attack success. However, studies show its effectiveness diminishes over time and should be repeated at least every six months.[8] Security teams should also routinely perform simulated phishing tests to identify weak points to focus on during future training sessions.

Use Email Security Controls

There are many programs and add-ons which an organization can deploy to help with phishing prevention. These may include security banners that highlight when an email from within the organization is actually from that person, maintaining a blacklist of malicious domains, and disabling macros on emails from non-trusted sources. By not putting the onus entirely on users, these solutions can make a positive difference as long as they don't lull your organization into complacency.

These measures — if followed faithfully — reduce the risk of a phishing attack and make it harder for criminals to break into your accounts. Unfortunately, determined hackers can still find a way.

THE MOST EFFECTIVE MITIGATION

Phishing is mainly about stealing passwords and credentials to gain access, so the only truly effective phishing prevention strategy is to eliminate passwords entirely. There is one sure way to do that.

Deploy Passwordless MFA

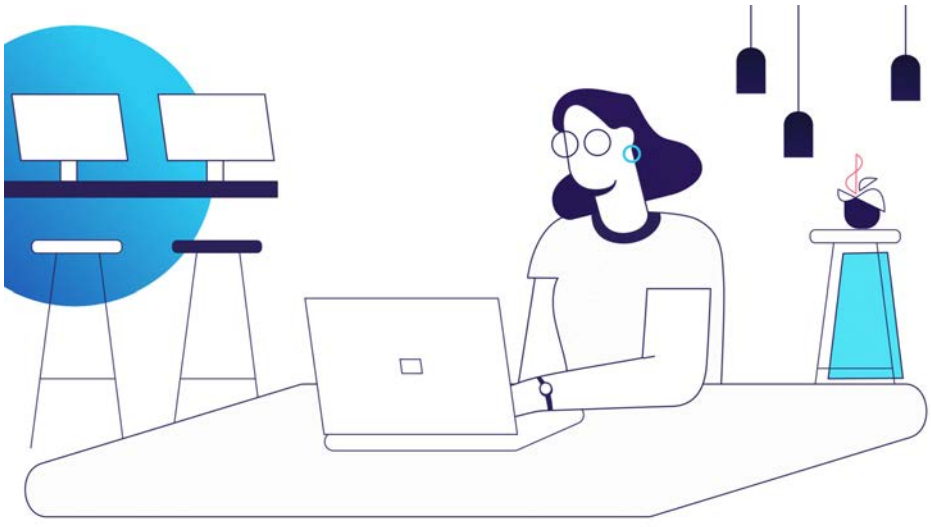
Passwordless MFA replaces passwords with an authentication system that does not rely on shared credentials or secrets that can be hacked. That's why the U.S. Office of Management and Budget recently issued guidance requiring phishing-resistant MFA to adhere to the Executive Order on Cybersecurity.[9] Other regulators, such as the Federal Financial Institutions Examination Council (FFIEC), have published similar requirements.[10]

Not All "Passwordless Solutions" Are Created Equal

Vendors have developed a variety of ways to enable passwordless authentication — some more secure than others. Look for a solution that bases its authentication protocols on Public Key Infrastructure (PKI). PKI-based systems completely eliminate OTPs, SMS tokens, or any kind of phishable credential. Instead, users confirm their identities through secure on-device methods, such as biometric sensors or decentralized PINs. These are used to unlock a private-public cryptographic key pair that has been generated and stored on the user's device. By removing shared credentials from the authentication process, these passwordless solutions render phishing attacks virtually useless.

Passwordless MFA Is Within Reach of Anyone

It used to be that passwordless MFA was only deployed by large companies that could afford the cost and implementation requirements. However, that situation has changed. There are now commercially available solutions that integrate with common SSO providers, making them easy and affordable for businesses of any size to deploy.



The Benefits of Passwordless MFA Go Beyond Phishing Prevention

Your top priority in adopting passwordless MFA is to eliminate the risk of phishing attacks. But there are significant, ancillary benefits to deploying passwordless MFA:

- **Users are more productive because system access is easier, and they don't get locked out due to password problems.**
- **Help desk resource requirements are reduced due to fewer password reset calls.**
- **IT staff is more productive and can devote more time to business-building work.**
- **Some solutions enable protection for both on-site and remote workers.**

Win the Phight

It's clear: Phishing attacks aren't going away, and attackers will continue to get more sophisticated in their efforts. As large corporations keep upping their security spend, criminals and other bad actors will increasingly aim their efforts at lower-profile, less well-protected organizations.

You can invest considerable time and effort trying to reduce the risk of a phishing attack and still have an unacceptable degree of vulnerability. By removing the most common attack vector — passwords — passwordless MFA provides the highest level of protection available.

HYPR is the leading provider of phishing-resistant True Passwordless™ MFA. To learn more, visit **hypr.com/smb** or sign up for a **demo**.

Sources

1 2021 Data Breach Investigations Report, Verizon, 2021

2 https://www.theverge.com/2020/7/30/21348974/twitter-spear-phishing-attack-bitcoin-scam

3 https://www.itpro.co.uk/security/ransomware/361853/ransomware-groups-will-target-smaller-businesses-in-2022

4 The 2021 Cost of Phishing Study, The Ponemon Institute, July, 2021

5 Internet Security Threat Report, Symantec, February, 2019

6 https://www.digitalinformationworld.com/2021/09/the-first-half-of-2021-saw-700-increase.html

7 https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-013a

8 An investigation of phishing awareness and education over time: When and how to best remind users, USENIX, August, 2020

9 Moving the U.S. Government Towards Zero Trust Cybersecurity Principles, Office of Management and Budget, September, 2021

10 Authentication and Access to Financial Institution Services and Systems, Federal Financial Institutions Examination Council, 2005