The Business Owner's Complete Guide to Phishing Attacks

Everything
you need to know
to keep your team
and data safe

brightflow
TECHNOLOGIES

Today, business owners must be aware of phishing attacks, what they look like, the damage they can do and how to prevent them while safeguarding your data.

Don’t take the bait: Start with this complete guide, which aims to educate you and your staff.

WHAT ARE PHISHING ATTACKS?

Phishing is a type of social engineering cyberattack that aims to have users divulge sensitive information, such as usernames, passwords, financial details or other personal data. These attacks typically involve fraudulent emails, messages or websites designed to mimic legitimate entities or communications.

Cybercriminals impersonate a trusted source to trick victims into opening an email, instant message or text message and then clicking on a malicious link. This action could result in the installation of harmful malware, a ransomware attack or the exposure of confidential information.

Phishing attacks typically begin with a seemingly harmless email, text message or phone call that appears to be from a trusted source, such as a reputable company or a known individual. This message or call usually contains a request or offers something enticing to lure the victim.

An attacker may craft a message that claims there’s a problem with your account or payment information, or they may offer a too-good-to-be-true deal to grab your attention. Phishing messages often contain a sense of urgency, compelling the recipients into immediate action, which may involve clicking on a link or opening an attachment.

When an unsuspecting user clicks on the link, it often leads to a fake website that mirrors a legitimate one. Here, the victims are prompted to enter sensitive information like login credentials, credit card details or other personal information. Attackers design these sites to collect and steal this entered data.

Alternatively, the link may prompt the user to download a file. This downloaded file could be malicious software or “malware” ready to infiltrate the user’s system and extract sensitive information or cause further damage.

PHISHING ATTACK SUCCESS RATES

The success rate of phishing attacks varies depending on factors such as the sophistication of the attack, the quality of the phishing email or website, and the awareness and vigilance of the targeted individuals.

In the recently released 2023 Internet Crime Report produced by the FBI's Internet Crime Complaint Center (IC3), the numbers confirm that cybercriminals continue to plague Americans by targeting U.S. networks, attacking critical infrastructure, holding our money and data for ransom, facilitating large-scale fraud schemes and threatening our national security.

IC3 received a total of 800,418 reported complaints, with losses exceeding $12.5 billion. This is an increase of 10% from 2022.

Phishing schemes were the number one crime type with over 298,000 complaints and investment schemes reported the highest financial loss to victims. Investment losses rose to $4.57 billion in 2023. Victims aged 30 to 49 were the largest reporting group for investment fraud.

> **In 2023, ransomware incidents continued to be impactful and costly.** After a brief downturn in 2022, ransomware incidents were again on the rise with over 2,825 complaints. This represents an increase of 18% from 2022. Reported losses rose 74%, from $34.3 million to $59.6 million. Cybercriminals continue to adjust their tactics, and the FBI has observed emerging ransomware trends, such as the deployment of multiple ransomware variants against the same victim and the use of data-destruction tactics to increase pressure on victims to negotiate."
>
> - FBI 2023 Internet Crime Report

+ **Phishing attacks** are one of the most common forms of cybercrime. In 2022 they increased by **48%** in the first half of the year.

+ **94% of firms experienced a phishing attack in 2023.**

\# The average global cost of a data breach caused by a phishing attack was **$4.45 million** in 2023.

* **28% of recipients opened** phishing emails, and **6% clicked** on malicious attachments or links.

+ **58% of organizations suffered account takeovers in 2023.**

+(Accessed 11 April 2024) InfoSecurity-Magazine.com *Verizon 2021 Data Breach Investigations Report #(Accessed 11 April 2024) Statista.com

COMMON ATTACK VECTORS

Phishing comes in a range of forms. Here are the most common:

Email phishing:

Fraudulent emails designed to trick recipients into clicking on malicious links, downloading attachments containing malware or divulging sensitive information.

Spear phishing:

Targeted phishing attacks that are customized for specific individuals or organizations, often using personalized information to increase credibility and effectiveness.

Whaling:

A subset of spear phishing, whaling specifically targets high-level executives and their assistants within an organization. These attacks aim to steal personal data or gain access to sensitive corporate information and often involve more advanced tactics due to the high-value targets.

URL phishing:

This is a form of phishing that involves the use of fraudulent URLs. Often these URLs are similar to those of legitimate websites, but with slight alterations or misspellings. Unsuspecting victims who click these URLs are then led to counterfeit sites where they are tricked into entering confidential information, which the attacker collects.

Smishing:

Phishing attacks conducted via SMS or text messages, where recipients are tricked into clicking on links or providing information through text-based communication.

Vishing:

Phishing attacks conducted over voice calls, where attackers impersonate legitimate entities, such as banks or government agencies, to deceive victims into revealing sensitive information.

Pharming:

Redirecting users from legitimate websites to fraudulent ones without their knowledge, often through manipulation of DNS settings or malware.

Social engineering:

In social engineering attacks, the attacker manipulates the user psychologically, often employing tactics that take advantage of previous cybersecurity training. It's akin to a con artist sweet-talking you into giving away confidential information. For instance, an attacker could email you pretending to be a disgruntled customer. In their complaint, they may include a malicious link, baiting you to click it to resolve the issue.

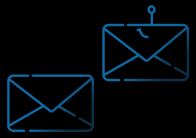
Or cybercriminals may message you masquerading as a popular service or bank. This is why it's critical to check and validate the source before clicking any links, even if they appear to be legitimate and from a trusted individual or brand.

Email spoofing:

With email spoofing, attackers create emails that seem to come from reputable sources, like your web hosting provider or a trusted contact. They forge the email header, masking their actual identity. This tactic can be an email that appears to be from your hosting company, prompting you to click a link or download an attachment. These actions may lead to unwanted malware or exposed personal data, so always verify the sender and be wary of suspicious emails.

Pop-up windows:

Cybercriminals can install pop-up windows on legitimate websites. An example would be a window popping up while you're entering data in your website's admin panel, asking for further authentication or additional details. Reputable services do not collect user data via pop-ups. Be cautious before sharing information this way.



Clone phishing:

Copies an email you may have already received and adds a message such as "resending this..." but it includes a link to malware.

Man in the middle attack:

A cybercriminal jumps into the middle of an existing email thread and takes over the conversation. They then ask you to take a specific action that will lead to a breach or ransomware attack.

Malware and ransomware:

Phishing emails may contain attachments or links that, when clicked, download malware onto the victim's device, allowing attackers to steal data or encrypt files for ransom.

IMPACT OF PHISHING ATTACKS

Phishing attacks can spell disaster for individuals and organizations alike. For individuals, an attack can lead to unauthorized purchases, stolen bank accounts or even identity theft. Phishing for corporations or government networks can lead to the distribution of malware, unauthorized access to secure data, financial losses and erosion of consumer trust and reputation.

WHAT SHOULD I DO IF I CLICK ON A PHISHING LINK AND ENTER MY INFORMATION?

If you have reason to believe that you're a victim of a phishing attack, it's essential to take quick action to limit the potential harm. Here are the recommended steps to take following a phishing attack:

- **Report the incident.** Flag any suspicious emails as phishing in your email client, which helps email providers identify and block such attempts in the future.
- **Notify relevant service providers.** If you clicked on a link or gave away your credentials, promptly notify the relevant organization or service provider. If you handed out financial account details, such as your credit card or banking information, get in touch with your bank immediately.
- **Change your passwords.** Changing your passwords promptly is crucial to preventing unauthorized access. If your email account credentials were compromised, this step becomes even more important because your email account can be used to reset other accounts' passwords.
- **Monitor your accounts.** Keep a close watch on your accounts for any suspicious activity. For example, set up website monitoring if you believe any of your website or cPanel accounts were affected. If you notice anything amiss or strange with your bank accounts, contact your bank immediately and report it.
- **Enable two factor authentication.** Enabling 2FA wherever possible will make it more difficult for the phisher to maintain unauthorized access to your accounts.
- **Update your software.** Ensure all antivirus applications, website software and third-party components are patched and up to date. Consider checking your website for malware if you believe your website accounts were affected. If you inadvertently downloaded malware to your computer, running an antivirus scan can help detect and remove it.
- **Contact local authorities.** In certain cases, reporting a phishing attack to your local law enforcement might be necessary, especially if you have suffered a financial loss due to fraud or identity theft.

Always remember to question unsolicited requests for your personal information, even if they appear to be from a legitimate source.

HOW DOES PHISHING AFFECT WEBSITE OWNERS?

As a website owner, you're RESPONSIBLE for safeguarding not just your website and data, but also your visitors' information.

Phishing can pose significant risks, including:

- **Unauthorized access to restricted areas.** If attackers gain your administrative login details via phishing, they can gain unauthorized access to your website. They can then manipulate content, inject malicious codes, steal valuable data or even lock you out of your own website.
- **Loss of personal or customer data.** Successful phishing attacks might lead to the loss of vital data. If you inadvertently reveal information related to your customers, this could lead to a breach of your customers' accounts. The loss of such critical data can lead to significant reputational damage and could have legal implications.
- **Hijacking your website for phishing attacks.** In some cases, phishing isn't intended to target you specifically but rather to gain access to your website's environment and use it for subsequent phishing attacks on users or customers. In essence, your website can become a launchpad for phishing, severely damaging your reputation and customer trust.
- **Compromised email accounts.** If your business emails fall into the wrong hands, it can lead to a direct conversation between the hacker (impersonating you or your staff) and your customers, possibly leading to broader data theft.
- **Damage to business reputation.** If your website becomes associated with phishing attacks, your brand reputation could take a major hit. This could lead to loss of business, as users might start to disassociate with your brand due to safety concerns.
- **Data breaches.** Phishing attacks can lead to data breaches, resulting in the exposure of sensitive information such as customer data, employee credentials or intellectual property.
- **Financial losses.** Phishing attacks can result in financial losses due to fraudulent transactions, unauthorized access to bank accounts or ransom payments to attackers.
- **Regulatory compliance violations.** Phishing attacks that lead to data breaches may result in regulatory fines and penalties for noncompliance with data protection laws such as GDPR or HIPAA.

OTHER DO'S & DON'TS TO STAY SAFE

- ✔ **DO hover your cursor over the sender's name in your emails**, as well as any website addresses. This will show you the actual email address used, or the website you're being directed to.
- ✘ **DON'T log in to any of your accounts by following a link in an email**. Go directly to the website that you always use and log in that way.
- ✔ **DO check all emails to make sure they're genuine**. Even if they're from close friends or colleagues.
- ✘ **DON'T use the same passwords across different online accounts.** Cyber criminals will often try your credentials on countless other sites once they've stolen them. Using different login details will keep your other accounts protected.
- ✔ **DO use a password manager** to make sure passwords are long and randomly generated, making them virtually impossible to guess.
- ✔ **DO implement multi-factor authentication** across applications (where you use a second device to prove it's really you logging in).

If you often deal with financial transactions over email, **it's a good idea to set up a dedicated email address that invoices should be sent to.** Don't advertise that address, making it far less likely that it will be targeted with phishing emails.

Another strategy is to **implement codewords with clients or suppliers if an email is regarding payments.** If the email doesn't contain the codeword, you know not to process the transaction. Don't email these codewords. Phone your suppliers to tell them about the codeword strategy.

Additionally, ensure your policies accurately reflect your stance on financial transactions and the best way to handle them. For example, you might decide that all transactions must be confirmed over the phone for security reasons.

PHISHING ATTACKS ARE CONSTANTLY EVOLVING

Phishing attacks pose a significant threat to businesses of all sizes, leading to data breaches, financial losses and reputational damage. By understanding the tactics and techniques used by attackers, implementing robust security measures and educating employees about best practices, businesses can mitigate the risk of falling victim to phishing attacks and protect their sensitive information and assets.

If you need help protecting your business, don't hesitate to contact your Jedi warriors at BrightFlow. We can help wrap a security force field around your team and your business.

brightflow TECHNOLOGIES

CALL: 704-585-1010
EMAIL: info@brightflow.net
WEBSITE: brightflow.net