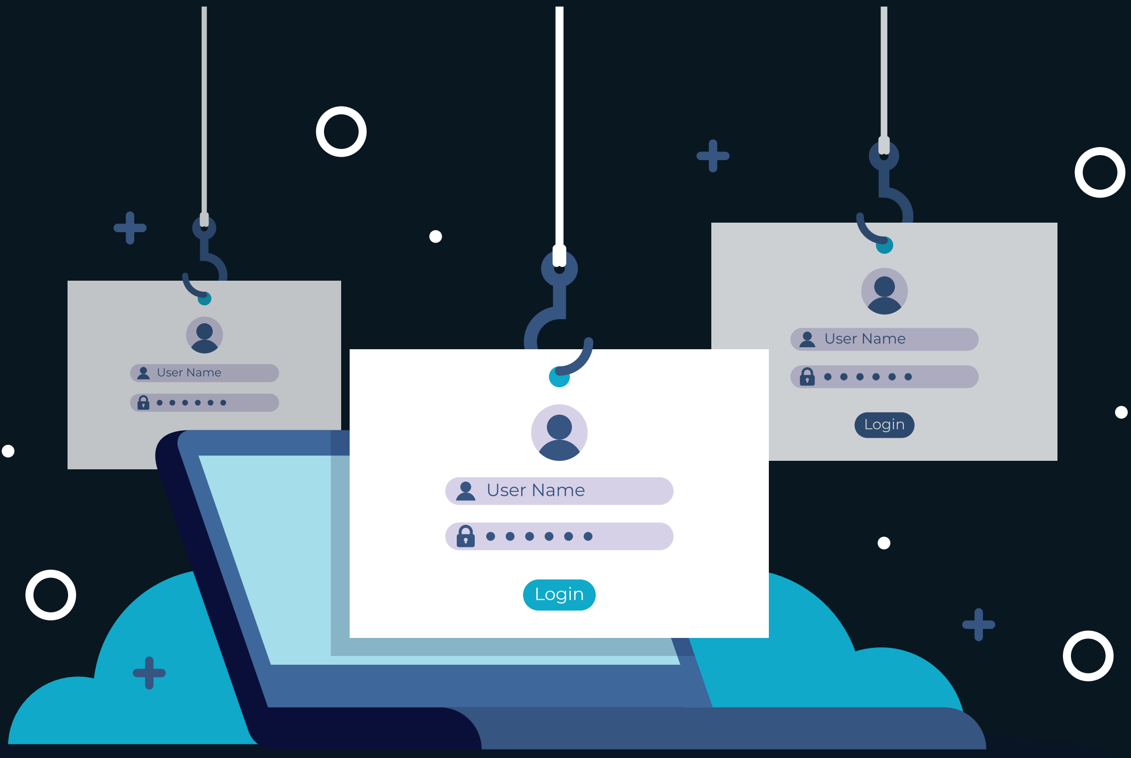
PROTECTED
HARBOR

PHISHING VS. VISHING

PROTECTING YOURSELF FROM CYBER THREAT



WWW.PROTECTEDHARBOR.COM

TABLE OF CONTENT

PHISHING VS. VISHING

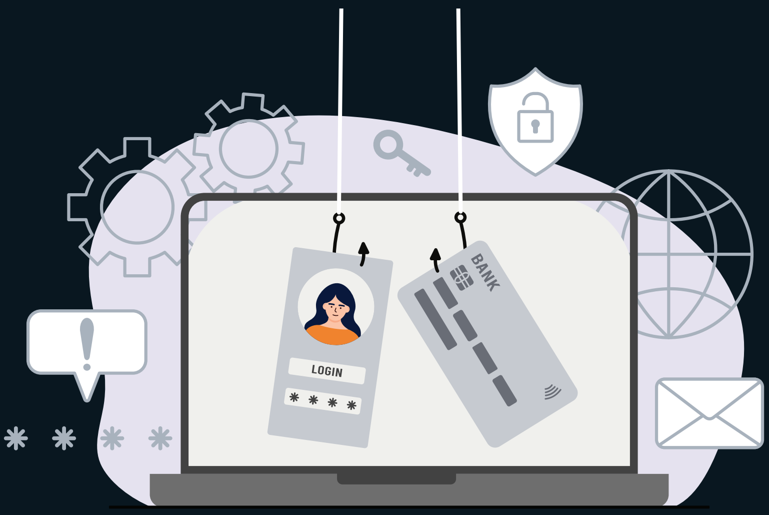
PROTECTING YOURSELF FROM CYBER THREATS

Cybercriminals are constantly evolving their tactics to deceive individuals and businesses into revealing sensitive information. Two of the most common methods used in these deceptive schemes are phishing and vishing. These forms of cyberattacks rely on social engineering techniques to exploit trust and manipulate victims into disclosing confidential data, such as login credentials, credit card numbers, or personal information.

Phishing involves sending fraudulent emails or messages that appear to come from legitimate sources like banks, online services, or government agencies. The goal is to lure victims into clicking malicious links or downloading harmful attachments, often leading to the theft of sensitive data or the installation of malware on their devices.

On the other hand, Vishing—a combination of "voice" and "phishing"—involves phone-based scams where attackers impersonate trusted entities, such as tech support or financial institutions, to trick victims into providing confidential information over the phone.

Both phishing and vishing are increasingly sophisticated and pose a significant threat to personal privacy, business security, and financial well-being. In this infographic, we'll explore the differences between these two threats, how they work, real-world statistics, warning signs to look out for, and tips to protect yourself from falling victim.



PHISHING

Phishing is a widespread and evolving form of cyberattack that targets individuals and organizations by disguising malicious communications as being from trustworthy sources. Attackers typically use email as their primary tool, although phishing attempts can also be delivered through social media, messaging apps, or fake websites.

The main goal of phishing is to trick recipients into sharing sensitive information such as:

- **Login credentials (usernames, passwords)**
- **Credit card details or bank information**
- **Personal identification numbers (PINs) or Social Security numbers**
- **Confidential company data**

Phishing emails or messages often appear to be from well-known institutions like banks, popular online services (e.g., PayPal, Amazon), government agencies, or even coworkers. They often convey a sense of urgency—such as claiming that your account has been compromised, you need to reset your password, or there's a financial transaction that requires immediate attention. Once victims click a malicious link or download an infected attachment, they are directed to fake websites designed to harvest their personal information or infect their systems with malware.

Key characteristics of phishing attacks:

- Impersonation: Attackers pretend to be someone or an entity the victim trusts.
- Sense of urgency: Often designed to pressure the victim into acting quickly without considering the risks.
- Malicious links or attachments: Links often lead to fraudulent websites, while attachments may contain malware.

Real-World Example:
A common phishing scam might look like an email from a popular bank informing you that there was suspicious activity on your account. The email contains a link that leads to a fake login page designed to steal your credentials when you enter them.

VISHING

Vishing, or voice phishing, is a type of phishing attack that uses the phone as the primary medium for deception. Just like phishing, vishing attempts to steal sensitive personal information, but instead of using emails or websites, the attacker uses voice calls. The scammer usually pretends to be from a legitimate organization, such as a bank, government office, or well-known company, and manipulates the victim into providing sensitive data, like account details, passwords, or social security numbers.

Vishing calls often involve sophisticated tactics to trick victims:

- Caller ID spoofing: Scammers can make it appear that they're calling from a legitimate number (e.g., a bank or government office), adding credibility to their claim.
- Social engineering: The attacker will use manipulative tactics such as pretending there's a problem with your account, offering a fake prize, or using threats (e.g., legal action, account closure) to get the victim to share information.

A common vishing scheme is the "tech support scam," where the caller pretends to be from a reputable tech company like Microsoft or Apple, warning you about a virus or technical issue on your computer. They instruct you to grant them remote access to your device, allowing them to steal sensitive information or install malware.

Key characteristics of vishing attacks:

- Impersonation: Attackers pose as customer support, government officials, or banking representatives.
- Pressure tactics: The victim is often threatened with consequences like legal action, account suspension, or fines.
- Sensitive information extraction: Victims are asked to provide personal details, account numbers, or passwords over the phone.

Real-World Example:

A common vishing scenario could involve a scammer calling you, pretending to be from your bank. They inform you of "suspicious activity" on your account and ask you to confirm your identity by providing your account number, PIN, or even passwords. The scammer might also ask you to perform a "security check" that involves revealing more sensitive data, leading to potential financial loss.

PHISHING

Over **3.4 billion phishing emails** are sent every day worldwide.

22% of data breaches in 2023 involved phishing.

Phishing attacks increased by 60% from 2022 to 2023.

83% of organizations experienced a successful phishing attack in 2023

VISHING

75% of businesses reported experiencing vishing attacks in 2023.

Financial fraud due to vishing cost businesses over **$2 billion** in 2023.

39% of vishing victims were aged 55 and above, making older adults a prime target.

Common Signs of Phishing and Vishing

- **Phishing Email Red Flags:**

  - Generic greetings like "Dear Customer."
  - Suspicious URLs or email addresses.
  - Urgency or threats (e.g., "Act Now!" or "Account Locked").

- **Vishing Call Red Flags:**

  - Unsolicited calls claiming to be from familiar companies.
  - Request for immediate action or payment over the phone.
  - Caller ID spoofing to mimic legitimate numbers.

HOW TO PROTECT YOURSELF

For Phishing:

• Verify the sender's email: Always double-check the sender’s email address to ensure it’s legitimate. Phishers often use slightly altered addresses that look real at first glance but contain subtle errors like misspellings or extra characters.

• Hover over links: Before clicking any links, hover your cursor over them to reveal the actual URL. Ensure the link leads to a legitimate website, and be wary of unfamiliar or shortened URLs.

• Use two-factor authentication (2FA): Enable 2FA on all accounts whenever possible. This adds an extra layer of security by requiring a second form of verification (like a code sent to your phone) in addition to your password.

For Vishing:

- Never provide sensitive information over the phone: Be cautious when asked for personal details over the phone. Legitimate companies rarely ask for sensitive information, such as account numbers or passwords, in unsolicited calls.

- Hang up and call back: If you receive a suspicious call, hang up and contact the organization directly using a number from their official website or a trusted source. This ensures you're speaking with a legitimate representative.

- Be wary of unsolicited offers or threats: Scammers often use pressure tactics, such as urgent requests or threats of legal action, to coerce you into giving up information. Take a moment to assess the situation before responding.

What To Do If You Fall Victim

Report the Incident:

- **Phishing:** If you receive a phishing email or accidentally click a suspicious link, report it to your IT department or anti-phishing services like Google Safe Browsing or Microsoft. Many email services also allow you to mark suspicious emails as phishing, helping to block future attempts.

- **Vishing:** If you’ve fallen for a vishing scam, immediately report it to your phone provider and, if necessary, to local authorities or anti-fraud organizations such as the Federal Trade Commission (FTC) or Action Fraud. If sensitive information was shared, notify the relevant institutions (e.g., your bank) to flag your account.

Take Immediate Action:

- **Change passwords:** If you suspect that your login credentials have been compromised, change your passwords for affected accounts right away. Use strong, unique passwords for each account, and enable two-factor authentication (2FA) for extra security.

- **Contact your bank:** If you shared financial information (credit card details, bank account numbers), reach out to your bank immediately. They can monitor your account for suspicious activity, freeze compromised accounts, and issue new cards if necessary.

Key Takeaways

- **Be skeptical of unsolicited messages and calls:** Whether it's an unexpected email, text, or phone call, always approach unsolicited communications with caution. Scammers often prey on trust and urgency, so take time to verify the sender or caller before responding.

- **Protect your sensitive information:** Use strong, unique passwords for each of your accounts and enable two-factor authentication (2FA) wherever possible. This adds an extra layer of security, making it harder for cybercriminals to access your information, even if your password is compromised.

- **Stay informed:** Cyber threats like phishing and vishing are constantly evolving. Regularly educate yourself and your employees on the latest tactics used by scammers, and ensure everyone knows how to spot and avoid these types of attacks.

Conclusion

In today's digital landscape, phishing and vishing attacks are more prevalent than ever, targeting individuals and businesses alike. Taking proactive steps—such as verifying communication sources, using strong security measures, and staying informed—can significantly reduce your risk of falling victim to these scams.

However, protecting your organization from these and other cyber threats requires a comprehensive approach to cybersecurity. By partnering with a trusted cybersecurity expert like Protected Harbor, you can ensure that your business is equipped with the tools and expertise needed to defend against cyberattacks. With proactive monitoring, advanced threat detection, employee training, and ongoing support, Protected Harbor can help you stay one step ahead of cybercriminals and keep your data safe.

PROTETED HARBOR CYBERSECURITY SERVICES

PROTECTED
HARBOR