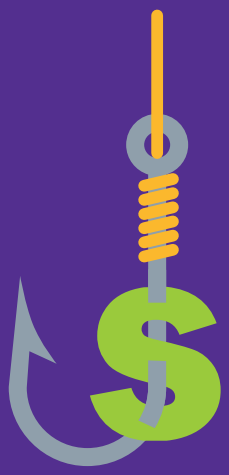

Phishing Scams:
How to Protect Your Organization from the Hook, Line, and Sinker

LeapFrog®

Phishing Scams: How to Protect Your Organization from the Hook, Line, and Sinker

Phishing scams began back with AOL, when the internet was just making its way into households. Today, they're still one of the most common methods used by cybercriminals to gain access to personal and financial data.

In 2023, phishing scams were the cause of 36% of data breaches, costing businesses nationwide over $2.7 billion.

What do the scammers want? To steal your personal information and login credentials, download malware (including ransomware), trick you into sending them money, and otherwise separate you from your valuables. It's what scammers do for a living.

Phishing scams are any attempt made to trick you into revealing sensitive information, such as passwords, personal identifiers, or financial information. Phishing can be in the form of emails, text messages, fake websites, and even phone calls.

What to look for – the current top scams

- Impersonation Scams appear to be from a personal or professional acquaintance asking for money or sensitive information
- A message to notify you about a delayed shipment
- Fake advertisements and/or digital storefronts offering heavy discounts
- QR Codes, typically on social media, that send you to a malicious website
- Fake contests and giveaways that require you to fill out an entry form or click on a malicious link to participate
- Romance scams where cybercriminals set up fake profiles and build relationships with victims, typically asking for money under false pretenses
- Cheap holiday and getaway deals
- Refund messages claiming you're owed money, requesting your personal information
- Debt Collector messages, claiming you owe money and often threatening actions if you don't pay
- "There's an issue with your account" messages requesting personal information to resolve the issue
- Heartstring scams that play on your emotions, fake GoFundMe accounts, fake non-profit organization websites and links, even missing kid/pet posts can have malicious links.

What to do if you suspect a Phishing Scam

- Slow down — look at emails carefully and, better yet, if you don't know the sender, don't look at them at all
- Do not click on suspicious links or open/download suspicious attachments
- Keep your personal information personal — never provide usernames, passwords, date of birth, social security number, credit card numbers, or financial information by email (or web pages linked to emails), even if the sender says it's urgent
- Verify the source by checking the email address, website URL, logo, and any other identifiers to make sure they are legitimate.
- If the message appears to be questionable, but from someone you know, call them directly to verify
- Inform your IT department if it's a work-related scam or you received the email at your work email address
- Verify organizations by navigating directly to their websites

Be sure to report scams to the FTC and file a complaint with the FBI to help stop fraudsters so they don't fool others. Afterward, delete any questionable message to ensure it doesn't get opened later.

How to protect your organization from phishing scams

Phishing scams are common and costly, so what can you do to decrease your organization's chance of being a victim?

88% of all data breaches are human error, and an estimated 45% of breaches involve internal actors, often tricked by phishing attacks.

- Educate, Educate, Educate: Regularly educate your employees to spot the latest scams and follow the best cybersecurity practices. Hiring a reputable outside company for training can be a great move. They will also often run phishing simulations to test employee awareness.
- Deploy security software: Utilize the most updated email authentication software, antivirus programs, and filters for spam and web browsing.
- Use multistep verification whenever available: If a phisher is able to get ahold of your login information, a second step verification will likely prevent access and bring awareness that you've been compromised.
- Implement security policies: Employees should know and utilize cybersecurity policies and procedures to address suspicious activity and threats.
- Monitor and report: If you see any fake websites or communications impersonating your company, immediately report them to your IT department, the FTC, and/or local law enforcement. Also, contact the registrar of the website and hosting provider to have the site removed.

Don't get tangled in the line of a phishing scam.

Taking preventative and proactive measures is a huge step in protecting your company from cyber-attacks. If you need support, reach out to a reputable and trustworthy company like Leapfrog to help manage your risks.

Leapfrog offers outsourced managed IT and cybersecurity services that fit easily into your business model. With over 25 years of MSP, MSSP, and CyberRisk Management experience, we help a broad array of companies simplify their IT operations while improving their security and resiliency. Our services are scalable, aligned, and built on a proven methodology, and our culture (we call it "Frogma") is built on Integrity, Service, and People so you get personalized, best-in-class support.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to take your IT and cybersecurity services to the next level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

© 2024 Leapfrog Services Inc. All rights reserved.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329