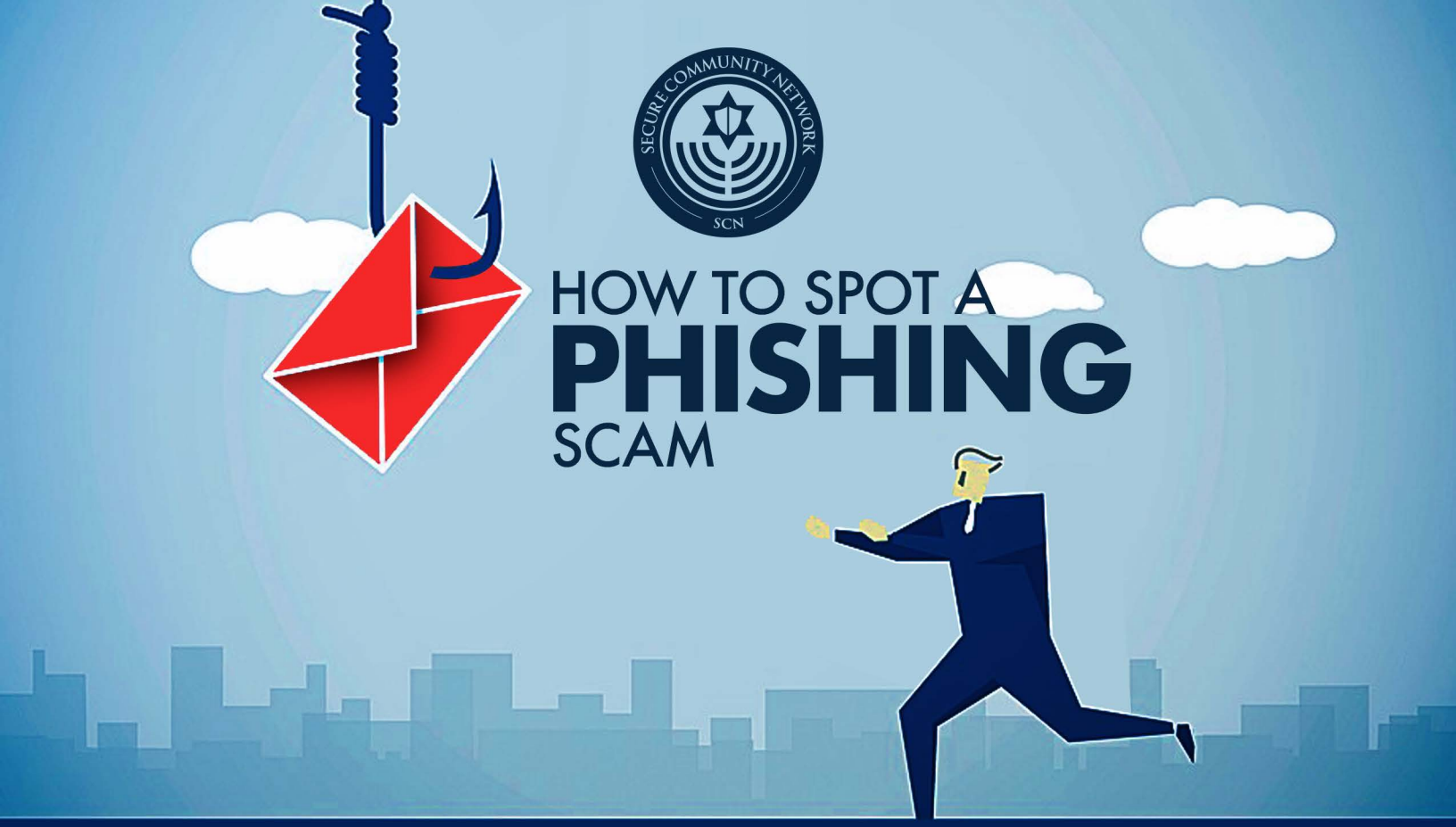


Phishing attacks are one of the most common forms of cybercrime and are a critical threat to any organization, especially as social engineering attacks become more sophisticated and difficult to identify. The best way to prevent a phishing attack is to know how to identify a phishing email.

BE CAUTIOUS OF GENERIC EMAILS
Always be wary of messages with generic subject lines or messages.

SUSPICIOUS URL
Hover over links included in emails to see the actual destination of the URL.

IMPROPER USE OF COPYRIGHT
Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately:
www.security.webmail.com.

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

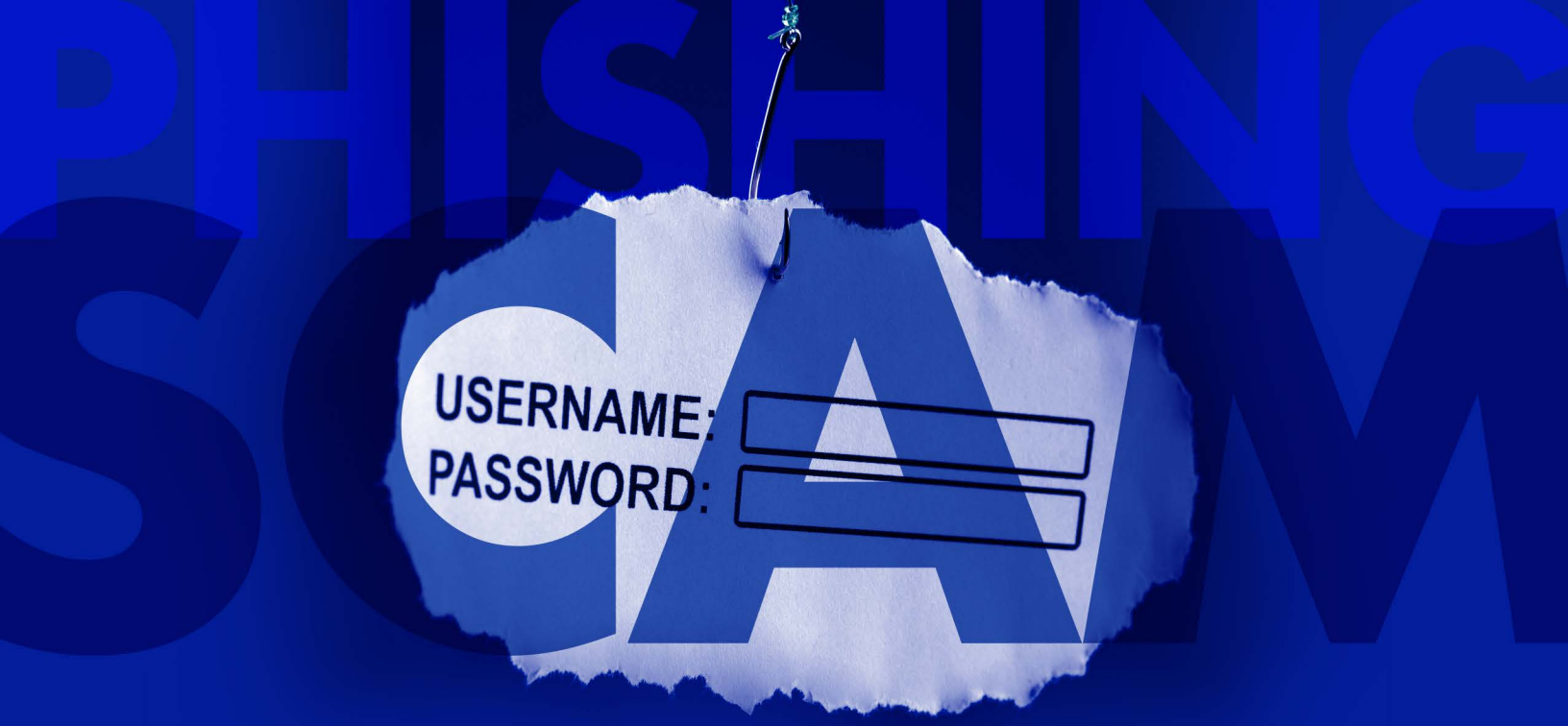
example-attachment.zip ()

BAD GRAMMAR/SPELLING
Phishing emails often contain misspelled words and bad grammar.

UNNECESSARY URGENCY
If something feels wrong, consider calling the organization or office directly to validate the email.

SUSPICOUS ATTACHMENT
Avoid opening attachments that seem suspicious or come from a sender you do not know.

"NCSAM Phishing Awareness 2017 Poster"
Department of Homeland Security, 25 September 2017



DECEPTIVE PHISHING

The most common form of phishing in which a cybercriminal impersonates a legitimate organization to lure the recipient into revealing sensitive information or click on a link/attachment that infects the user's computer with malicious code.

SPEAR PHISHING

Spear phishing is when a cybercriminal targets specific individuals in a phishing attempt. Cybercriminals may gather personal information about their target – often using information gleaned from social media – to customize the phishing attempt.

WHALING

Whaling is similar to spear phishing, only the target is bigger; in whaling attacks the cybercriminal targets executive officers or senior managers in an organization.Whaling emails are often customized – frequently containing personal information and company logos.

OTHER METHODS

The widespread use of Dropbox and Google Docs by organizations has led cyber criminals to customize their attacks to target users of these platforms. Voice phishing – or vishing – is when a fraudster uses the phone to solicit sensitive information instead of email.

Bisson, David. "6 Common Phishing Attacks and How to Protect Against Them" Tripwire, 5 June 2016

PHISHING PREVENTION TIPS

Simple best practices to help prevent you or your organization from falling victim to a phishing attack include:

Make passwords long & strong:
Combine capital and lowercase letters with numbers and symbols to create a more secure password. Change passwords periodically.

Use stronger authentication:
A stronger authentication helps verify a user has authorized access to an online account.

Be cautious of what you share on social media:
Consider only connecting with people you already know. Be sure to use privacy settings on all social media and accounts. Cybercriminals often get information from online profiles and social media, using that information to make their phishing attack more convincing and increase their chances of tricking their target.

Use secure, traceable transactions:
Be conscious when sharing payment information online. Avoid using prepaid money cards, wire transfers, or other non-traditional payment methods.

Install & update anti-virus software:
Regularly update antivirus software, firewalls, email filters, and anti-spyware.

When in doubt, throw it out:
Links in email and online posts are often how cybercriminals compromise your computer. If it looks suspicious – even if you believe you know the source – it's best to delete or, if appropriate, mark it as *"junk email."*

To report a cybersecurity threat or incident, please contact:
SCN Duty Desk at 844.SCN.DESK
or email DutyDesk@SecureCommunityNetwork.org

"Phishing Tip Card," Department of Homeland Security, accessed 22 March 2018

"10 Steps to Avoid Scams," Better Business Bureau, accessed 22 March 2018