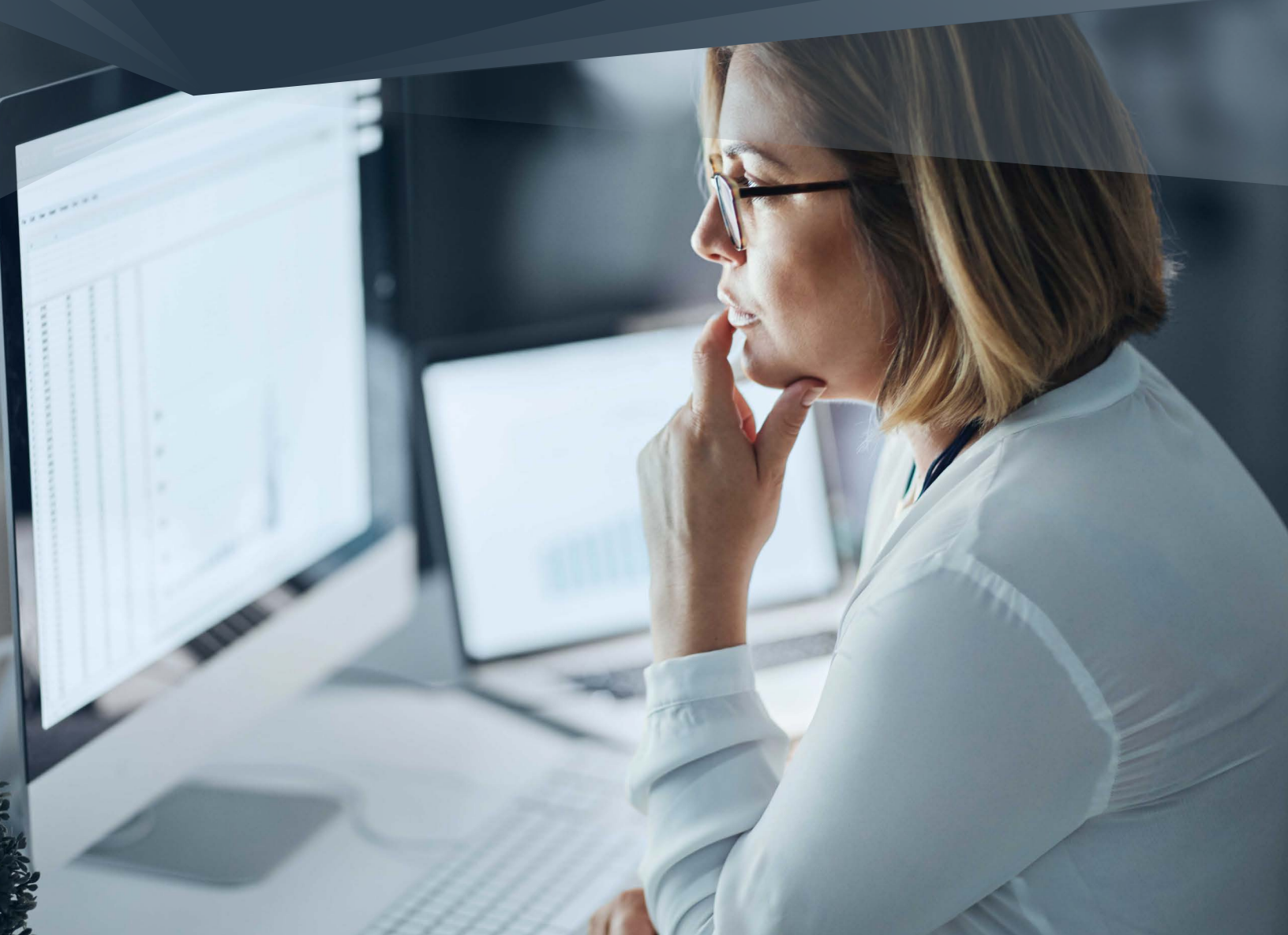
FORTINET

EXCLUSIVE NETWORKS

EDUCATION GUIDE

What Is Phishing



Executive Summary

Phishing, a form of cyberattack based on social engineering, is the top security risk for organizations today. Phishing techniques range from mass email blasts and text messages to targeted attacks against individuals with highly valuable information. Counterfeit websites play a prominent role in phishing exploits, imitating trusted websites and companies to instill confidence in potential victims.

Organizations can defend against phishing attacks with email security solutions and web address filtering. However, the most effective countermeasure is a trained and diligent employee. Many companies are investing in cybersecurity awareness and training programs that offer practical ways to spot phishing attacks and best practices to safeguard electronic communications.

What Is Phishing?

Phishing is a form of social engineering in which an attacker masquerades as a trustworthy entity and tries to persuade, scare, or threaten the recipient to take a specific action or reveal personal information that leads to a security compromise. Phishing attacks use email, text messages, social media posts, voice communications, and other media. Often, they contain links to counterfeit websites designed to trick them into revealing sensitive information such as usernames, passwords, account numbers, and credit card details.

More than a decade after its first appearance, phishing remains the most common type of cyberattack. In a recent survey, 96% of organizations say that email phishing scams pose the biggest security risk, followed by end-user carelessness (76%) and social engineering (70%).[2] Supporting this finding, a detailed analysis of 750 security incidents found that phishing was the top category (37%).[3]

Who Is at Risk?

Virtually anyone in the organization who uses email, texting, instant messaging, social media, or voice communications is a potential phishing victim. In the past, attackers sent out thousands or millions of phishing emails in the hope of snaring a few victims. Recent years have seen a shift to more targeted techniques such as spear phishing and voice phishing (vishing).

Today, phishing attacks increasingly target executives, both because their contact information is often publicly accessible, and they are more likely to possess valuable data. Cyber criminals then use stolen email credentials from the executive to send authentic-looking messages requesting employees to wire money to offshore accounts or commit other kinds of fraud.

Executives see phishing as the number one cybersecurity threat to their organizations.[1]

Most Valuable Information to Cyberattackers

1. Customer information
2. Financial information
3. Strategic plans
4. Board member information
5. Customer passwords
6. R&D information
7. M&A information
8. Intellectual property (IP)
9. Nonpatented IP
10. Supplier information[4]

Business email compromise (BEC), a scam involving unauthorized wire transfer, accounted for more than $1.2 billion in losses last year.[5]

What Kinds of Phishing Attacks Are There?

While not a comprehensive list, the following exploits are some of the more common phishing techniques that cyberattackers employ:

Email Phishing

Phishing emails, where attackers pose as trusted colleagues or other "known" contacts to trick unwary employees and contractors into handing over passwords or other details, are easy to send and hard to combat. The success of these exploits depends on how closely the phishing email resembles official correspondence through the use of logos, taglines, and brand graphics. Users with training in security awareness can foil many phishing attacks by spotting clues such as fake URLs in embedded links (Figure 1).

Spear Phishing

Where general phishing attacks use spam-like tactics to blast thousands at a time, spear-phishing emails target specific individuals within an organization. In this type of scam, hackers customize their phishing emails with the target's name, title, work phone number, and other information to trick the recipient into believing that they have a connection with the sender. Spear phishing is the method of choice for criminal organizations and state actors who have the resources needed to research and implement these more sophisticated attacks. In addition, most ransomware attacks use spear phishing to deliver their malware (see "Ransomware: Phishing's Costly Payload").

Whaling

Whaling is a variant of spear phishing that targets CEOs and other executives and is increasingly a phishing exploit of cyber criminals. As these contacts typically have unfettered access to sensitive corporation secrets, the risk-reward is dramatically greater.

Ransomware: Phishing's Costly Payload

Ransomware is a form of malware that prevents users from accessing their system or personal files until they pay a ransom, usually via cryptocurrency or credit card. Ransomware attacks are usually delivered through phishing attacks via injected attachments or links to spoofed websites. The average ransom increased 89% in the first quarter of 2019 to $12,752, while the average cost in downtime from a ransomware attack was $64,645.[7]

Cities and municipalities are a frequent target. According to FBI and the United States Department of Homeland Security, more than 50 cities, large and small, have been hit with ransomware attacks, including Atlanta, which cost the city $17 million. The healthcare industry is also becoming a soft target for phishing attacks and ransomware.[8]

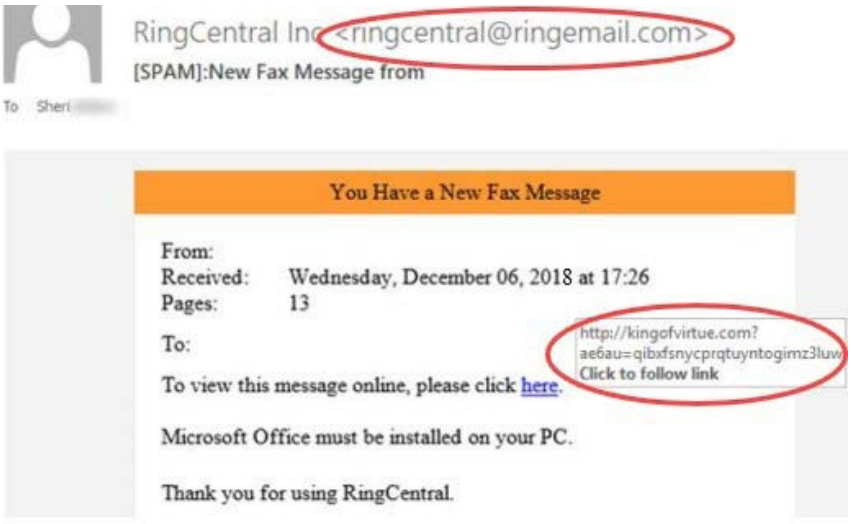


Figure 1. Phishing email with fake URL link. Note the discrepancy between the purported source URL ringemail.com (top) and the true source URL kingofvirtue.com (bottom).[6]

Baiting

Baiting is a technique that offers something of interest to the victim as a way to trick the user into opening an infected attachment. Recent attacks have used emotionally charged political and social issues to lure victims into security breaches. In one well-known

incident, attackers launched a spear-phishing campaign timed with the release of a whistleblower memoir involving national security issues. The email, written in various languages, includes a Microsoft Word attachment that purports to be the text of the book. However, in reality, it contains the Emotet Trojan virus.[9]

Spoofed Websites

Attackers create spoofed websites to collect sensitive information or launch malware attacks such as ransomware. These sites are designed to mimic a familiar internet site (e.g., bank, credit union, government agency, or trusted vendor) to lure the visitor into a false sense of security.

To help avoid these imposter sites, cybersecurity training encourages employees and contractors to trust only secure URLs starting with https and displaying the lock icon in the web browser address bar, which indicates that the site supports encrypted communications. However, this method is not foolproof. Recently, hackers spoofed a United Nations website, including the security information (Figure 2).

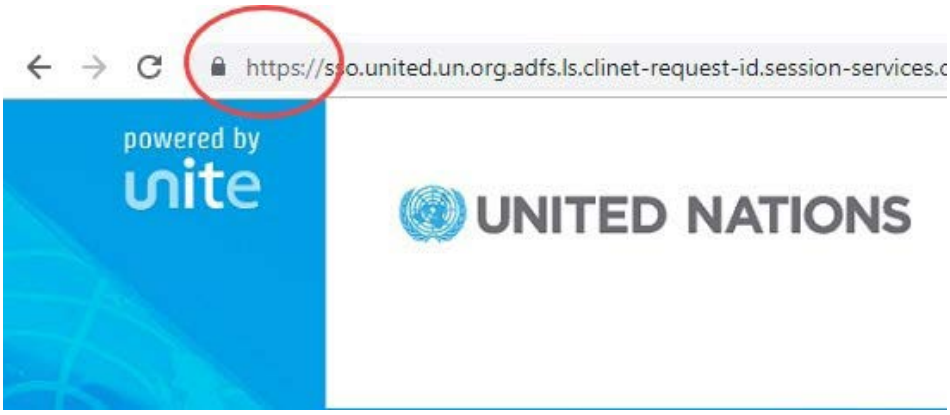


Figure 2. Spoofed website. Note the presence of the lock icon and https//.

SMS Phishing (Smishing)

Mobile devices are increasingly becoming the targets of smishing attacks, a variation of phishing using SMS text messaging. As in other phishing attacks, criminals masquerade as government workers, tech support representatives, or financial institutions to lure people into divulging personal information. One reason for the increase in smishing is that smartphone users tend to trust text messages more than phone calls or emails.[10] In particular, employees, contractors, or just individual consumers are often distracted when a message arrives. This increases the likelihood that the recipient will click on a dangerous link without thinking. Smartphones have blurred the lines between business and personal lives, which allows attackers to enter via relatively insecure personal apps and thereby gain access to business information.

Voice Phishing (Vishing)

Just as experienced debt collectors can persuade consumers to divulge financial information, skillful criminals can attack organizations using a technique called voice phishing or vishing. In one recent kind of vishing attack, the scammer fraudulently displays the FBI's real telephone number on the victim's caller ID to entice the recipient to answer the call. The scammer then impersonates a government official and uses intimidation tactics to demand payment of money purportedly owed to the government.[12]

Tech Support Scams

Tech support fraud continues to be a growing problem. As the name suggests, scammers pose as tech support engineers, either working for a victim's organization or for an independent service. In one variation, the attacker lures victims with emails

In 2018, the Federal Trade Commission logged 93,331 complaints about unwanted text messages, including smishing attempts, up 30% from the year before.[11]

Last year, the U.S. Federal Bureau of Investigation received 14,408 complaints related to tech support fraud from victims in 48 countries.[13]

containing realistic-looking URLS such as **yourhelpteam.support.** The scammer then persuades the victim to enable remote access, which the attacker uses to steal credit card numbers, usernames and passwords, and other personal information.

What are Effective Phishing Defenses?

To be effective, anti-phishing programs need to include three primary components: cybersecurity awareness and training, email security, and web address filtering.

Cybersecurity Awareness and Training

While employee behavior can contribute to the problem of phishing, it can also constitute an important part of the solution. Staff members first detected and reported the most disruptive breaches 63% of the time.[14] Security leaders recognize the importance of security awareness training. More than half of organizations indicate implementing security awareness training for IT departments and end-users is high on their list of priorities.[15]

For security leaders evaluating their cybersecurity awareness programs, the following are some of the key areas to evaluate:

- Establish metrics for behavior change such as numbers of security-related help-desk tickets and users falling for phishing schemes
- Survey the workforce to measure motivation, ability, and triggers to find out what employees actually know and how inclined they are to act on that knowledge
- Repeat the survey regularly to measure trends

Email Security

Email security is a mature market with many available choices. There are still "pure-play" email security vendors, security vendors offering broad portfolios and suites, and even infrastructure companies that offer solutions. Regardless of vendor type, email security must provide three basic capabilities when it comes to stopping phishing attacks:

- Address the risk posed by a constantly changing and accelerating threat landscape
- Help organizations move from a reactive to a more proactive security posture
- Provide a quantifiable return on investment (ROI)

Web Address Filtering

Web address filtering (WAF) limits access based on a database of known information about specific websites. WAF solutions either permit access to known safe sites (whitelisting) or prohibit access to sites used in phishing and malware attacks (blacklisting). Because of the dynamic nature of malicious websites, top-tier WAF solutions use machine learning and threat intelligence subscription services to stay current.

Signs of Phishing Emails

Phishing attacks are highly variable and increasingly sophisticated. There are signs, however, that can alert users to a possible threat:

- **Generic salutations.** Most legitimate companies address the recipient by name, so phrases such as "Dear account holder" or "Dear valued customer" should be suspect.
- **Requests for sensitive information.** No reputable business today would send an email asking the recipient to reply with login credentials, credit card numbers, or account numbers.
- **Unusual requests from executives.** A recent trend involves an authentic-looking email from an executive requesting the recipient to contribute to a charity or even conduct a wire transfer in the person's absence.
- **Suspicious-looking domain names.** Many phishing attacks come from domains that look familiar but in fact are subtly different from the legitimate business. A common approach is to substitute numbers for letters, such as paypa1.com versus paypal.com.
- **Unsolicited attachments.** Emails with unsolicited attachments are often the work of cyberattackers. Most legitimate businesses send links to downloads.

How Can Organizations Stop Phishing Attacks?

To prevent successful phishing attacks, the following actions are recommended:

- Institute programs for employee cybersecurity awareness and training and continually measure their effectiveness
- Procure secure web gateways featuring web attacks with URL filtering, visibility, and secure sockets layer (SSL) and transport layer security (TLS) inspection
- Ensure the email security system is validated by third-party independent testers
- Notify employees immediately as specific phishing exploits are detected

- Enable multi-factor authentication, prioritizing accounts with access to sensitive data
- Set alerts to identify suspicious activity such as authentication from IP addresses in high-risk regions, mail forwarding, and legacy connection protocols
- Enforce account lockout after a specific number of failed attempts[16]

[1] "Is cybersecurity about more than protection?" EY Global Information Security Survey, 2018–19.

[2] "KNOWBE4 2019 Security Threats and Trends Report," KnowBe4, Inc., October 2019.

[3] "Managing Enterprise Risks in a Digital World," BakerHostetler, 2019.

[4] "Phishing: Don't Be Phooled! 2018 Public-Private Analytic Exchange Program," U.S. Department of Homeland Security, 2018.

[5] "2018 Internet Crime Report," FBI Internet Crime Complaint Center, 2019.

[6] "Phishing: Don't Be Phooled! 2018 Public-Private Analytic Exchange Program," U.S. Department of Homeland Security, 2018.

[7] Lisa O'Reilly, "As Ransomware Grows, the Need for Phishing Threat Prevention Becomes Paramount," Security Boulevard, August 20, 2019.

[8] Ibid.

[9] "FortiGuard Threat Intelligence Brief," FortiGuard Labs, September 27, 2019.

[10] Octavio Blanco, "Smishing: A Silly Word for a Serious Fraud Risk," Consumer Reports, September 19, 2019.

[11] Ibid.

[12] "FBI Warns of Scammers Spoofing FBI Phone Numbers in Southern California to Trick Victims Using Threats, Intimidation," FBI Los Angeles, August 15, 2019.

[13] "2018 Internet Crime Report," FBI Internet Crime Complaint Center, 2019.

[14] Steve Ranger, "Phishing attacks are a worse security nightmare than ransomware or hacking," ZDNet, April c, 2019.

[15] "KNOWBE4 2019 Security Threats and Trends Report," KnowBe4, Inc., October 2019.

[16] Ibid.

November 2, 2019 7:31 AM

505974-0-0-EN

D:\Fortinet\White Paper\Phishing Education\eg-FA-guide-on-phishing