



# **SANS Institute**

## Information Security Reading Room

# **Defend Your Business Against Phishing**

---

Matt Bromiley

Copyright SANS Institute 2019. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Defend Your Business Against Phishing

Written by **Matt Bromiley**

January 2019

Sponsored by:  
**Microsoft**

### Phishing for Your Business

It's time to talk about a favorite pastime of cybercriminals: phishing. Phishing is an ever-evolving and widespread method of attack against small and medium-sized businesses. Why? Because it's easy to deploy, can target any business with an email address or phone (everyone), and has a high rate of success and impact.

Fortunately, many businesses have found that they can increase protections against phishing campaigns without harming their day-to-day operations. No matter how well a cybercriminal may plan a phishing attack, it only works if you, the victim, are unprepared. It's time to turn the tables with proven strategies to mitigate these types of attacks in the future.

In this paper, we will get you on the right path to defend against phishing attacks. We'll begin by examining sample phishing tactics, so you can get familiar with some techniques that attackers commonly use. Then, we'll focus on defenses and provide actionable steps you can take *today* to start defending against phishing campaigns—no matter your budget or level of expertise.



#### Phishing Facts

**Phishing:** a trick, delivered by email, messages, phone calls or snail mail, to entice users to do something they ordinarily would not do:

- Click a malicious link
- Provide personal information
- Hand over authentication credentials

In a 2018 survey conducted by Bredin, 24 percent of small and medium-sized businesses said phishing was the No. 1 cybersecurity threat to their networks.<sup>1</sup>

<sup>1</sup> SMB Pulse Survey, April 2018, [www-cdn.webroot.com/5715/3728/5184/Webroot-SMB-Pulse-Survey-9-18-18.pdf](http://www-cdn.webroot.com/5715/3728/5184/Webroot-SMB-Pulse-Survey-9-18-18.pdf)



Our goal is to arm businesses of all sizes with the knowledge and capabilities to increase their phishing defenses, often using technology that's already in place. We also want to empower your employees to better recognize phishing attempts so as to not take the bait. As you'll see, phishing defense doesn't have to be tough or expensive.

## Phishing: A Primer

Before we can discuss defenses, we must first understand what a phishing attack looks like. By understanding some of the key attributes that attackers use when they craft a phishing email, phishing becomes easier to spot—and of course, easier to thwart.

### Phishing Defined

In its simplest form, phishing is a trick to get users to do something they otherwise would not do—click a malicious link, answer a question to provide personal details or provide their username and password to a suspicious person. The term *phishing* is often synonymous with spoofed emails, but attackers also use instant and text messages, phone calls and even snail mail. Regardless of *how* the phish is delivered, many defenses against phishing remain the same.

The success rate of phishing often depends on the way the message is crafted and delivered. Messages often prey on human nature—attackers are assuming that if they can craft just the right message or send it to enough people, someone will let them in. After all, who doesn't want to win a free cruise, see pictures of their friends or read an encrypted document from a trusted colleague?

### Detecting a Phishing Email Message

There are often telltale signs you and your employees can use to detect when a message is legitimate and when someone is trying to exploit your human nature.

Let's look at a sample phishing email to understand some of the techniques attackers will use. Before you read the explanation on the next page, see if you can pinpoint what each number in Figure 1 is calling out.

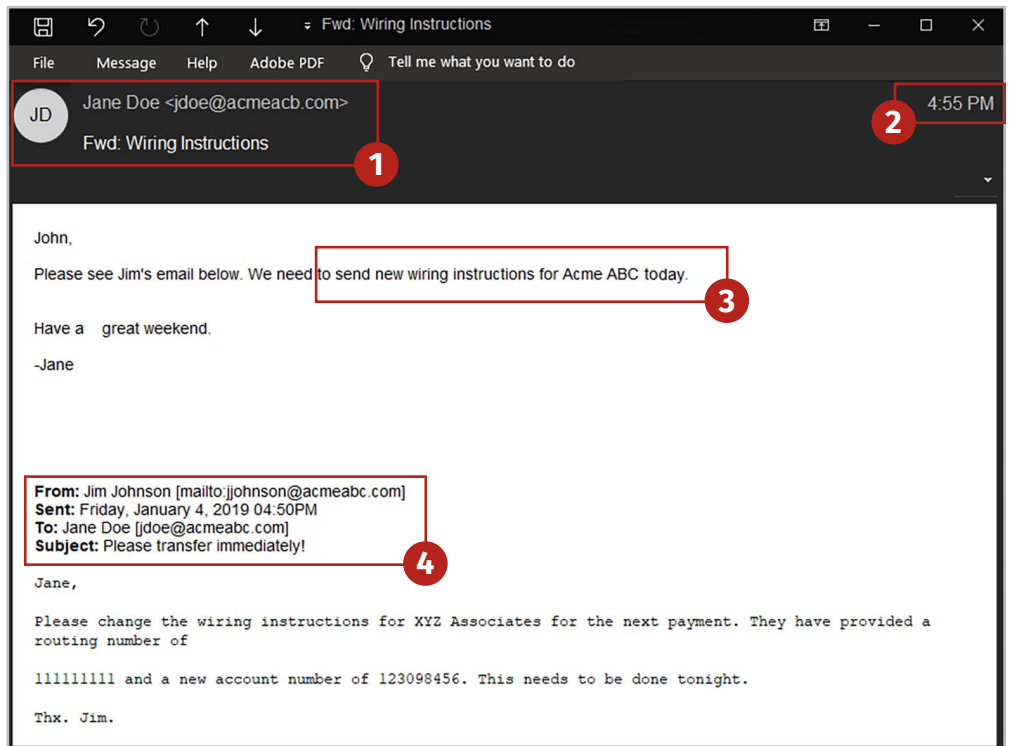


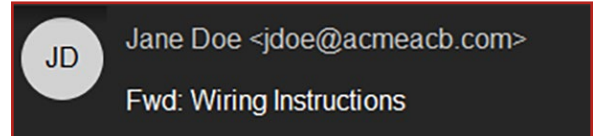
Figure 1. Sample Phishing Request for ACH Transfer Changes

Despite how simple it may seem, the sample email in Figure 1 resembles a business email compromise (BEC) phish such as those used to steal more than \$12 billion from businesses around the globe over the past half-decade.<sup>2</sup>

<sup>2</sup> Federal Bureau of Investigation, "Business E-Mail Compromise the 12 Billion Dollar Scam," July 12, 2018, [www.ic3.gov/media/2018/180712.aspx](http://www.ic3.gov/media/2018/180712.aspx)

Let's examine the key points of this email and see how many can be faked.

1 While attackers must send their emails from the outside, they want their message to look as if it's coming from a trusted source. There are two ways to achieve this:



- a. Attackers can spoof the email headers, which makes the email look like it's coming from a different source. This tactic is tough for employees to spot, but relatively easy for email security tools to detect. (The next section describes these user defenses.)
- b. Some attackers register domains that look *almost* identical to your company domain and then send emails to your users from there. Did you catch the difference between **acmeabc.com** and **acmeacb.com**? If your inbox receives lots of emails in a day, it can be tough to catch the difference. Most people don't even read all of their incoming email addresses!

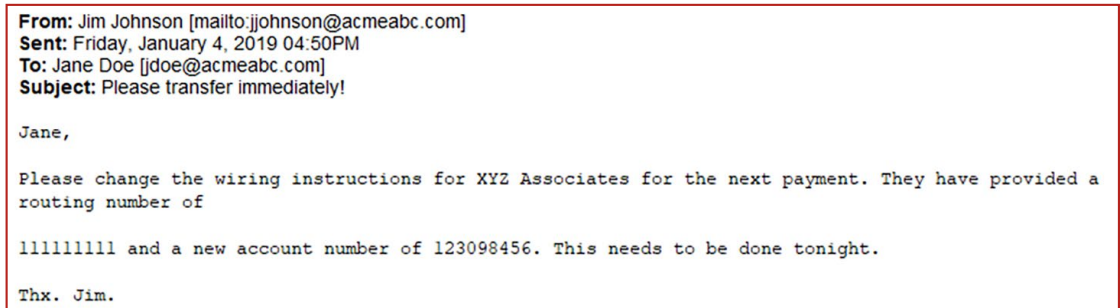
2 Sometimes attackers send phishing emails at moments when they know employees are rushed, busy or overworked. They know that targets are more likely to click when they are in a hurry. This email was sent late on a Friday afternoon, near the end of the month. A member of the accounting staff—the intended recipient—is likely busy closing out the end-of-month financials and not paying attention to details within this email.

4:55 PM

3 Attackers often impose a sense of urgency with their emails. "Please do this now!" or "This is urgent!" will make your employees think it's a pressing matter. Again, if attackers can impart a sense of urgency, employees are less likely to pay attention to the signs of a phishing attack.

to send new wiring instructions for Acme ABC today.

4 Did you notice that this email looks like a forwarded message? That's a fake! Another technique attackers use when they craft phishing emails is to insert details that make it seem like the email originated from a trusted source.



When we walk through these attacker techniques, some seem simple and obvious. Others may be harder to detect, but it is not impossible.

## Other Phishing Formats

While it's important to understand how email phishing may be constructed, remember that phishing can also extend to other formats. You or your colleagues may also be victim to phishing instant messages, text messages, phone calls or snail mail letters. While the delivery medium may differ, the goal is the same: to get the users to provide information that they may otherwise not want or intend to provide.

In the next section, we'll discuss techniques that you can use to defend against phishing attempts of all kinds.

# Implementing Phishing Defenses

The best defenses against phishing are two things organizations likely already have: technology and users. This section examines how to use each to your advantage and prevent phishing attacks from compromising your business.

## Technology: The First Line of Defense

Your first line of defense is to use technology to flag, prevent and highlight potential phishing emails. Before you get out the checkbook, be aware that you may already have some of these capabilities! Table 1 describes key technology defenses that organizations can use to defend against phishes.

**Table 1. Technology Defenses**

Technique	How Does It Defend?	How Can I Implement It?
Use multifactor authentication (MFA).	MFA provides a second step of authentication over and above a username and password that requires users to input a PIN code or some other value. Many attackers will be unable to get this data and will be stopped in their tracks.	You may already have MFA and not be aware. Many cloud-based email solutions currently offer MFA; it simply needs to be enabled.  If MFA is not available, you can usually implement it for a low per-person cost.
Approach links and attachments with caution.	This technique is a combination of user and technology that recommends zero trust on all hyperlinks and/or attachments that come through emails. Users should approach these with caution and hover over links to view the true path of the URL. Don't open attachments if they are asking you to do something odd, such as enabling scripts or macros.  If it looks suspicious, don't click it!	You can implement this practice for free! Make sure users know that they can get information about suspicious items without needing to click or open them. (For more information, see the next section on user education.)
Flag external emails.	Many email solutions can also be used to flag emails that are coming from external sources. They will often append the words [EXTERNAL] or EXT to the email subject, which lets the recipient know that the email is from a sender who is outside the user's organization.	Depending on your email provider, you may be able to turn this feature on for free.  If not, you can usually—for a low cost—implement an email gateway that will compare addresses and mark external emails for you.
Keep software updated.	Attackers sometimes craft phishes to take advantage of vulnerable software on your users' systems. Keep software patched and updated, and the threat is neutralized.	Free! If you own software, such as operating systems or office productivity suites, make sure you update it regularly. Many vendors offer automatic updates as they fix potential vulnerabilities. Be sure you sign up for them.  If you are using free software, such as a web browser, make sure it is patched regularly.

Even the best-laid defenses can be thwarted by attackers—and sometimes they are successful. It may be helpful to take your technological defenses to the next level and generate alerts that identify external links or suspicious activity. This technique can also help defend your users who are reading email from other platforms, such as tablets or mobile phones.

## Users: Your Last—and Strongest!—Line of Defense

One of the easiest-to-implement—and most resilient—assets to combat phishing is your users. Because users are the targets of phishing attacks, they are typically the last line of defense. Don't leave user training to chance—make this work in your favor!

### Train Your Users

Practice makes perfect, right? One of the best ways to ensure that your users are current on phishing detection is to schedule time for training and review. Successful organizations will have regular phishing trainings, sometimes performed on a monthly or quarterly basis, where simulated phishing emails are sent to staff to see how many users fall for the bait. This gives management a chance to ensure that training is working and users are vigilant about suspicious emails.




The other benefit to having regular phishing training is to ensure that your users know what to do when they receive a suspicious email. For example, your organization may have one or more IT security people who should be alerted to suspicious emails so they can investigate further. Even in smaller businesses, where there may be only a handful of employees, knowing what and when to say something may prevent other users from falling victim as well. Of course, the safest action—regardless of organization size—is not to open!


*One of the easiest-to-implement—and most resilient—assets to combat phishing is your users.*


Also, consider adding phishing to your orientation agenda for new staff—you don't want an employee's first week to be marred by a successful phishing attack.


### Key Training Tips

To strengthen user defenses, educate your users to be wary of the following common issues and train them to implement these best practices:

-  **Trust your instincts.** If you have received an email that seems out of place, like an odd request that is out of character for the supposed sender, you're likely correct. *Never hesitate to follow up verbally with a coworker on a request such as opening an encrypted document or wiring money.*
-  **Double-check every link.** It's not uncommon to receive hyperlinks in an email. However, double-check each one before you click. Hover over the link for a brief second and make sure the URL is what you expect it to be. If you are unsure, don't click. Verify.
-  **Be careful with email attachments.** Attackers may also send attachments, such as document or spreadsheet files, that contain malicious code. Be careful of attachments that require you to allow running of macros, which may run untrusted code on your computer.

 **Add multi-touch verifications for important transactions.** Important transactions, such as money transfers or account changes, should have multiple stages of verification. One of the more common attack techniques is to reroute funds destined for a legitimate payment. Adding another verification step in the process involves another person, which provides an additional point of clarification—and lowers the chance of fraud.

 **Audit your own accounts.** Double-check your account to make sure that there are no forwarding rules or other suspicious items that *you did not create* in place. Even if an attacker has your credentials, their success is predicated on staying hidden in plain sight. Scheduled account audits can help spot potentially concerning activity.

 **Don't provide your username and password to an email form.** If you receive an email asking you to log in before you do anything else, stop and double-check the request. Third-party sites, such as encrypted documents or file transfer services, **DO NOT NEED** your corporate username and account to work. These requests should ask you to create new credentials.

## Conclusion

With all the threatening statistics, phishing can seem impossible to defend against. However, if you lean a little on available technology and ensure that your users are informed and well-trained, you can significantly reduce the risk of a successful attack that disrupts your business and your bottom line. Tell cybercriminals you won't take the bait!

Phishing attacks are often simple attacks that seek to take advantage of human nature and get employees to provide data that they otherwise might not feel comfortable sharing. Attackers are hoping you'll fall for their tricks, but easy-to-implement defenses and educated users are the best lines of defense. See the next page for a reproducible handout that you can give your employees today to help mitigate phishing.



## Defend Against Phishing

### **Follow your gut.**

If it doesn't look right, verify.

### **Implement multifactor authentication.**

One of the best phishing defenses is to implement multifactor authentication, requiring users to enter a PIN code or other value, which limits attackers' capabilities even if they have your credentials.

### **Let technology do the work.**

Your email solution can likely flag external emails and provide strong authentication. Let it do the heavy lifting.

### **Keep your technology updated.**

Phishers like to take advantage of outdated software. Keep your software up to date, and you'll be fine.

### **It's not just emails: Watch other mediums too!**

Phishes can arrive in multiple forms. Be as diligent in your texts, direct messages, snail mail and phone calls as you are in your emails.

©2019 SANS Institute. This page may be copied for distribution to employees for use in phishing education.



## About the Author

**Matt Bromiley** is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

## Sponsor

**SANS would like to thank this paper's sponsor:**





# Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS 2019	Orlando, FLUS	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS Cyber Security Middle East Summit	Abu Dhabi, AE	Apr 04, 2019 - Apr 11, 2019	Live Event
SANS London April 2019	London, GB	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KYUS	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, SA	Apr 13, 2019 - Apr 18, 2019	Live Event
SANS Boston Spring 2019	Boston, MAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
SANS Seattle Spring 2019	Seattle, WAUS	Apr 14, 2019 - Apr 19, 2019	Live Event
FOR498 Battlefield Forensics Beta 1	Arlington, VAUS	Apr 15, 2019 - Apr 20, 2019	Live Event
SANS FOR585 Madrid April 2019 (in Spanish)	Madrid, ES	Apr 22, 2019 - Apr 27, 2019	Live Event
SANS Northern Virginia- Alexandria 2019	Alexandria, VAUS	Apr 23, 2019 - Apr 28, 2019	Live Event
SANS Muscat April 2019	Muscat, OM	Apr 27, 2019 - May 02, 2019	Live Event
SANS Pen Test Austin 2019	Austin, TXUS	Apr 29, 2019 - May 04, 2019	Live Event
Cloud Security Summit & Training 2019	San Jose, CAUS	Apr 29, 2019 - May 06, 2019	Live Event
SANS Bucharest May 2019	Bucharest, RO	May 06, 2019 - May 11, 2019	Live Event
SANS Security West 2019	San Diego, CAUS	May 09, 2019 - May 16, 2019	Live Event
SANS Perth 2019	Perth, AU	May 13, 2019 - May 18, 2019	Live Event
SANS Milan May 2019	Milan, IT	May 13, 2019 - May 18, 2019	Live Event
SANS Dublin May 2019	Dublin, IE	May 13, 2019 - May 18, 2019	Live Event
SANS Stockholm May 2019	Stockholm, SE	May 13, 2019 - May 18, 2019	Live Event
SANS Northern VA Spring- Reston 2019	Reston, VAUS	May 19, 2019 - May 24, 2019	Live Event
SANS New Orleans 2019	New Orleans, LAUS	May 19, 2019 - May 24, 2019	Live Event
SANS Autumn Sydney 2019	Sydney, AU	May 20, 2019 - May 25, 2019	Live Event
SANS MGT516 Beta Two 2019	San Francisco, CAUS	May 20, 2019 - May 24, 2019	Live Event
SANS Amsterdam May 2019	Amsterdam, NL	May 20, 2019 - May 25, 2019	Live Event
SANS Hong Kong 2019	Hong Kong, HK	May 20, 2019 - May 25, 2019	Live Event
SANS Krakow May 2019	Krakow, PL	May 27, 2019 - Jun 01, 2019	Live Event
SANS Atlanta 2019	Atlanta, GAUS	May 28, 2019 - Jun 02, 2019	Live Event
SANS San Antonio 2019	San Antonio, TXUS	May 28, 2019 - Jun 02, 2019	Live Event
Security Writing NYC: SEC402 Beta 2	New York, NYUS	Jun 01, 2019 - Jun 02, 2019	Live Event
SANS Jeddah March 2019	OnlineSA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced