ROI TECHNOLOGY INC.

# Phishing Attacks: How to Recognize Them and Keep Your Business Safe

Cybercrime is on the rise, and hackers are using any opportunity to take advantage of an unknowing victim to gain access to personal information for financial gain. The new "work from anywhere" world puts everyone at risk of cyber-attacks.

One commonly used tactic is phishing. Phishing messages are crafted with the end goal of capturing a person or an organization's sensitive data. If your employees fall prey to phishing scams, it can affect your company network by transferring malware and viruses over internet connections.

One phishing email has the power to cause downtime for your entire business and, unfortunately, costs small businesses on average $53,987. As the scams get more sophisticated, they get harder to detect. Prepare your team for the next phishing threat by learning how to spot phishing schemes before they become a problem.

## Here are five different types of phishing attacks to avoid:

### 1. Mass Campaigns

Wide net phishing emails are sent to the masses from a knock-off corporate entity asking them to enter their credentials or credit card details. Attacks that rely on email spoofing appear as if a trusted sender sent them, but there are few telltale signs to look for:

- Does the information given look legitimate? Look to identify things like misspellings or a sender email address that have the wrong domain.
- Review the message for any logos that look odd or fake.
- Ignore emails that have only an image and very little text.

### 2. Spear Phishing

Directly targets a specific organization or person with tailored phishing emails.

- Look out for internal requests from people in other departments or seem out of the ordinary for the job function.
- Be wary of links to documents stored on shared drives like Google Suite, O365, and Dropbox because these can redirect to a fake, malicious website.
- Any documents that require a user login ID and password may be an attempt to steal credentials.
- Don't click a link from an alleged known website. Instead, go to the browser, and go to the website yourself. This way, you can be sure you're getting to the right website and not a phishing one.

### 3. Whaling

Whaling refers to spear-phishing attacks directed specifically at senior executives and other high-profile targets in an attempt to gain access to company platforms or financial information.

- If a senior leadership member has never made contact before, be wary of taking the requested action.
- Make sure that any request that appears normal is sent to a work email, not personal.
- If the request seems urgent, it might be costly if it is fake. Send a separate email/text or call the recipient and verify his request. Better safe than sorry.

### 4. Clone Phishing

The attacker copies a legitimate email message sent from a trusted organization and replaces a link that redirects to a malicious/fake website.

- Be wary of unexpected emails from a service provider, even one that might be part of everyday communication.
- Look out for emails requesting personal information that the service provider never asked for. If you know the request is legitimate, it is best to go to the browser and type the data directly to the website.

### 5. Pretexting

Pretexting involves an attacker doing something via a non-email channel (e.g., voicemail) to set an expectation that they'll be sending something seemingly legitimate shortly only to send an email that contains malicious links.

## What to do if you think you've received a phishing email?

**Social engineering** is "the psychological manipulation of people into performing actions or divulging confidential information." Malicious actors will use every trick in the book to get people to open an email, click on links, or take other actions. Examples of social engineering when it comes to phishing emails include:

- Asking you to click something to get something.
- Corporate entities insisting a password needs to be updated or credit card information is outdated.
- Using a sense of urgency.
- Offering you something that you were not expecting.

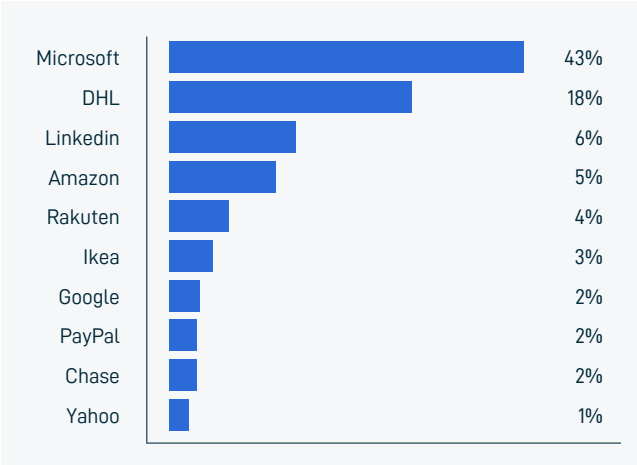
**Is the email real, or just trying to look real?** Look for clues, many of which can be found in the email itself.

- Check the sender's actual email address.
- Look for odd grammar or spelling mistakes.
- Unexpected sender.

**If you clicked through to the webpage:**

- Is the URL aligned with the webpage brand?
- Does it look like the actual webpage you were expecting?
- Pay attention to its structure, colors, other pages within the site, and the main menu.
- Be extra cautious with the following brands:

**Top brands ranked by their overall appearance in brand phishing attempts in in Q4 2020:**




Source: *CheckPoint*

**Be careful!** Phishing scammers are impersonating file sync and share platforms and sharing fake documents or folders in an attempt to infect your computer.

Email is still the most popular form of communication in a business context, and phishing emails threaten organizations of all sizes and types. Learning how to recognize a phishing email is critical for keeping yourself and your organization protected.

### Stop Phishing before it starts!

Coaching your employees on how to spot phishing scams is important, but sooner or later someone is likely to get fooled. Talk to us to learn how automated scanning of Microsoft 365 email and collaboration tools can stop these hacks before they get started.