TECHVERA

The Ultimate Guide to Phishing Scams for SMBs

Cybersecurity

Table of Contents

How does phishing work?

FW: THANKS VERY MUCH FOR YOUR MAIL///this is a scam...they're using military people now???? - Me

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: Capt. George Hunter
To: Marine Cpl Motivated
Cc:
Subject: FW: THANKS VERY MUCH FOR YOUR MAIL///this is a scam...they're using military people now????
Signed By: cghunter13@gmail.com

From: CAPT.GEORGE HUNTER US MARINE [mailto:cghunter13@googlemail.com]
Sent: Saturday, May 10, 2008 1:54 PM
Subject: THANKS VERY MUCH FOR YOUR MAIL

Dear Friend.

Thanks for your mail and for accepting my offer. I apologize for my late reply, it was due to the fact that I was in the line of duty. Since your last email to me on the month of December 2007, I could not reply back because my troops were camping at the road to the Jordanian border that makes it difficult for me to check my mails.

I am ready now to transfer the money to you after due consideration. The total amount is $6.8 million United States Dollars inside the 2 boxes. I want you to send your bank account details to enable me transfer the money immediately. This transfer will be done through the Bank of Baghdad, Iraq, to your corresponding bank.This will not be sent once, I will transfer $1,000,000 dollars in each transfer.

When this transfer is completed, you will take 50% of the money as your percentage and deposit the rest in your bank for me. I am giving you all the trust and I believe that with the help of God, we will successfully transfer this money out of Iraq. Please do not disclose this deal to anybody as to protect my duty with the US Marine. I took my picture which is in attached file below for your confirmation. I also have my ID Card and Drivers License as backup proof.

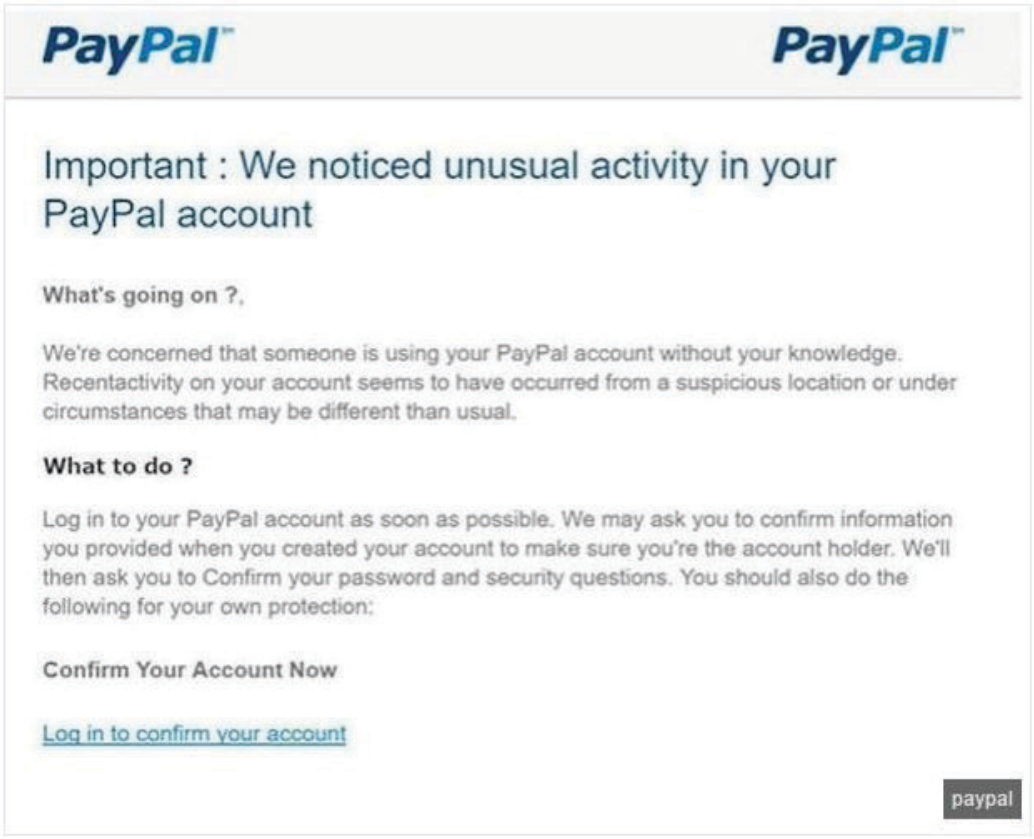
I will be waiting to hear from you as soon as possible to proceed. Always contact me through my private email:capt_hunter_g@yahoo.com
<mailto:email%3Acapt_hunter_g@yahoo.com>

Example of an older phishing scam email via Defense.gov

Phishing scams consist of an attacker who sends messages through email, SMS, or over the phone designed to trick the recipient into giving away sensitive information. They will try to convince you they are from a legitimate source, such as your bank or subscription services.

Attackers want to fool you into taking a desired action – entering your login information onto a phony login page, "confirming" your credit card details for a popular service, or wiring money to them as they pretend to be one of your vendors.

Most attackers used the "spray and pray" method in the past, blasting out thousands of messages at once in hopes a few people would fall for it. Malicious messages were easy to identify as they were created quickly, and contained giveaways like grammatical errors and broken English, things that no legitimate service would send out.


PayPal PayPal

Important : We noticed unusual activity in your PayPal account

What's going on ?,

We're concerned that someone is using your PayPal account without your knowledge. Recentactivity on your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.

What to do ?

Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to Confirm your password and security questions. You should also do the following for your own protection:

Confirm Your Account Now

Log in to confirm your account

paypal

Now criminals have realized people are harder to fool as the public becomes more educated in scams. They're constantly trying new, more advanced methods to get what they want. Some attacks are designed purposely for an organization after the attacker thoroughly researches their target. Phishing emails are crafted carefully and formatted just like the real deal, becoming even more difficult to distinguish.

Some scams fall out of favor after a few years, but phishing is just getting more popular. "Microsoft's Security team analyzes more than 6.5 trillion security signals a day to identify trends that could affect the digital landscape that we all live in. After scanning more than 470 billion email messages that have been sent and received by customers of its Office 365 platform, the company reports that malicious phishing attacks are on the rise, and not by a small margin — by a massive 250 percent. Worse, techniques used by scammers are becoming more proficient and harder to detect." (Digital Trends)

As phishing becomes smarter, so must its targets!

Who is behind phishing scams?

There are hundreds, if not thousands, of people and groups behind various phishing scams. Many are never brought to justice, so it's difficult to say where most are coming from.

Cybercrime is a massive business, and oftentimes there are groups of people working together to perpetrate attacks. The end goal is most often money. There have been a few discoveries in the last few years that give us an idea of who is behind phishing scams and why:

This phishing scam group built a list of 50,000 execs to target (ZDNet)

From the article: "[The phishing group] London Blue operates like a modern corporation. Its members carry out specialized functions including business intelligence (lead generation), sales management (assignment of leads), email marketing (semi-customized BEC attack emails), sales (the con itself, conducted with individual attention to the victim), financial operations (receiving, moving and extracting the funds), and human resources (recruiting and managing money mules),"

Turkish Group Using Phishing Emails to Hijack Popular Instagram Profiles (Dark Reading)

From the article: "A group of Turkish-speaking hackers is hijacking popular Instagram profiles, including those belonging to actors and singers, and, in some cases, promising to turn back control to the victims in exchange for a ransom or nude photos and videos.

Researchers from Trend Micro say they have recently observed several incidents where the group has been using a phishing scam to take over the Instagram profiles of people with between 15,000 and 70,000 followers. They have subsequently changed the primary contact information associated with the breached accounts to lock the original owners out.

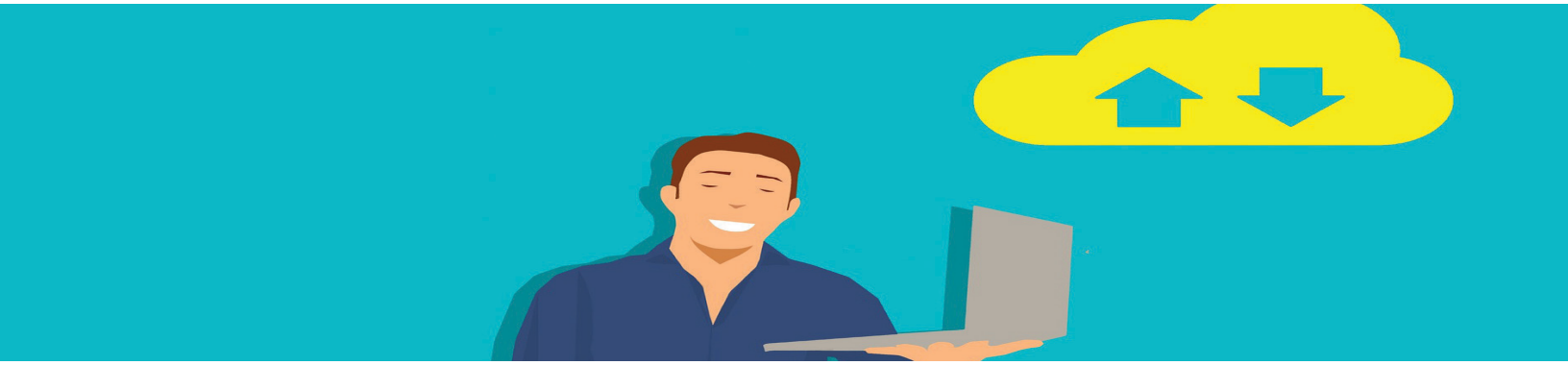
The victims have ranged from famous personalities to owners of small businesses like photo equipment rental stores, [Trend Micro] said in a report released Thursday."

Attackers often congregate on the Dark Web, where they will share techniques, stolen information, and malware to help their cause.

Find out if your business' information is for sale on the Dark Web

TECHVERA

Common types of phishing attacks targeted at SMBs



SaaS Grab

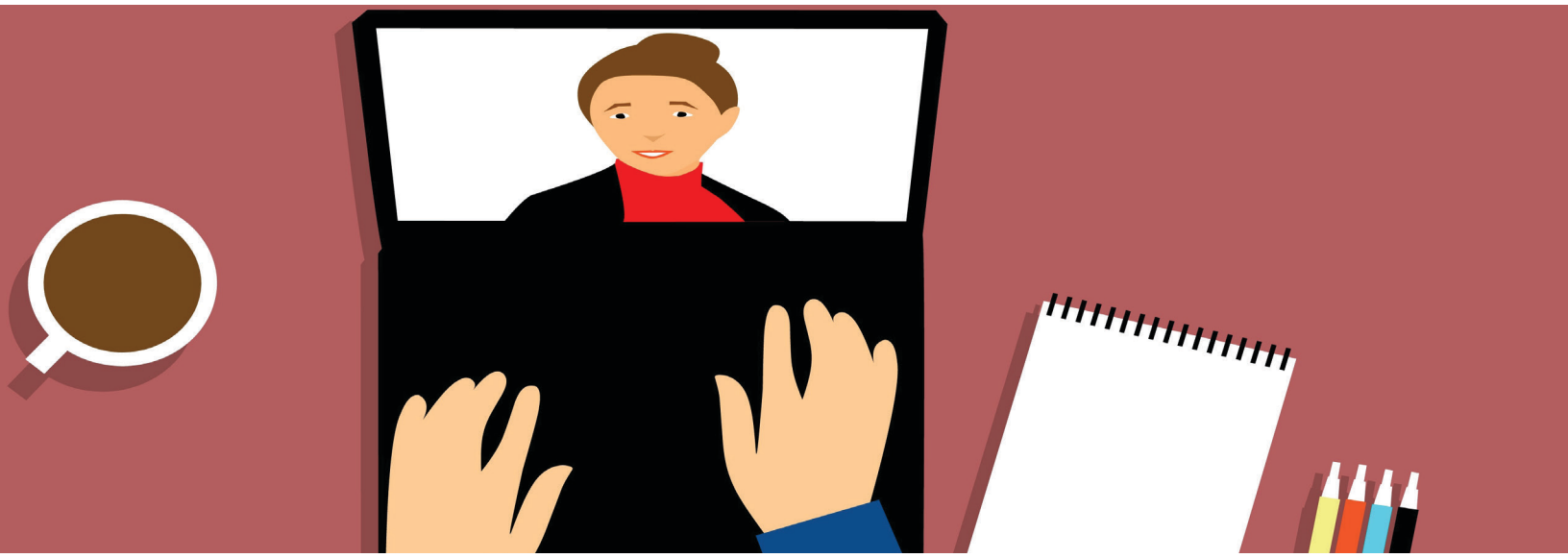
With many businesses relying on cloud services such as Office 365, G Suite, Dropbox, and Slack, hackers know there's huge potential in gaining access to just one account in a company network. Phishing emails in this category will generally attempt to lead you to a fake login page for one of these services. By pretending there was a security incident you need to review, an important notification, or an expired password, they incite urgency and bring your guard down.

If an attacker can gain access to a team member's account, they can send out phony emails to contacts to get even more information, impersonate the victim, attempt wire fraud, find credentials for and request password resets on other accounts, and gain access to company files.

Best way to avoid: Enable multi-factor (2FA) authentication on any accounts that allow it.

Do not click links or open attachments in emails from services you use unless you 100% trust the sender and were expecting the email. Most reputable companies like Microsoft and Google will not send clickable links or attachments unrequested through email and they will never ask for your personal information.

If you think something's up with an account, go directly to the service's website yourself from your web browser and log in without following links from the email.



Mixed Messages

Online messaging apps have given attackers another way besides email to scam their victims. Malicious messages will be sent through Facebook, Microsoft Teams, Skype, etc. These platforms generally don't have the same security or filtering options seen in business email.

Recipients are more likely to click a link or open a file in these programs because while they've been trained to be suspicious of emails, messaging platforms haven't received the same attention.

Best way to avoid: Train employees to use caution with any messaging platform, and make them aware that cybercriminals are utilizing these apps. Some third-party tools also exist to help secure online messaging programs.

TECHVERA

Let's (Business Email) Compromise

BEC attacks are on the rise as a successful one can easily net hundreds of thousands or even millions of dollars in one swoop for the perpetrator. "According to CNBC, law enforcement agencies have dealt with over 17,000 victims who have collectively lost more than $2.3 billion to BEC attacks." (VadeSecure)

Sometimes you'll hear this referred to as CEO, wire fraud, or invoice phishing. By compromising an executive's email account, an attacker can dupe another employee (usually a financial manager) into wiring money to them. This is easily accomplished by going through old messages, finding a vendor the company's previously sent money to, and changing only the routing/account information. Most people won't check that the account numbers match previous payments and will send the money right off to the criminal's account.

The rise of social media and large-scale data breaches have made these attacks more effective in recent years. A criminal can easily find a company's hierarchy and personal information on social media. Coupled with credentials found through data breaches, it's all too easy for an attacker to convincingly impersonate and/or take over the account of someone at your business.

Best way to avoid: Many banks, especially business banks, will allow you to set up extra security features before they process any transfer or vendor payment. Examples include sending a code to your email or phone as in two-factor authentication, creating a pin or password, and requiring two people at your company to approve the order.

We also recommend requiring something like this internally regardless of your bank setup. If a request comes through email, have that employee confirm the request through a different channel i.e. text, phone call, in person, or a messaging program.

TECHVERA

Sharing Isn't Caring

Attackers are figuring out ways to circumvent email security features like scanning for malicious links. Criminals will embed dangerous files within sharing services like Dropbox or Google Drive, then send a link to that file to the victim.

Since the link within the message is from a reputable service, most security filtering settings won't flag it. But once the victim follows the link and falls for the scam, their information can be stolen, malware installed on their machine, etc.

Best way to avoid: As always, never click links in emails unless you were expecting it! Confirm with the person who appears to have sent the message through an alternate channel – phone, in person, text.

TECHVERA

Kill Bill

This email is a common target for both businesses and consumers. It will attempt to convince you that there's been a billing issue with a service you use – Netflix, Paypal, Quickbooks, etc. Just click the link in the email to verify your information and it will all be cleared up! Or, more likely, you'll send your financial, login, and/or personal information straight to the perpetrator.

Best way to avoid: Once again, NEVER follow links from emails you aren't expecting. If you want to check the validity of an email like this, call the company directly or visit the website and login from your web browser. If there is a billing issue, you'll be able to see straight away.

Companies are aware that phishing scams like this are prevalent, and will generally never ask you to follow a link or confirm personal information from an email.

Taxation Without Representation

Tax season is, of course, when this scam is at its peak and it comes in a few flavors. Some emails will state that you're eligible to receive a refund, or that you will be audited. Both want you to give up personal information.

In another variation, an attacker will pretend to be from a vendor or adviser and attempt to "confirm" employee tax information.

Best way to avoid: The IRS will pretty much always send you important information through snail mail. They will never ask you to confirm personal or financial details over email or even the phone.

If a vendor or adviser calls or emails trying to get employee information, have a system in place to confirm these requests before giving anything out. This could entail channeling everything through your CEO or another person who is familiar with all your vendors, and/or requiring all requests be made via certified mail.

How to spot a phishing scam

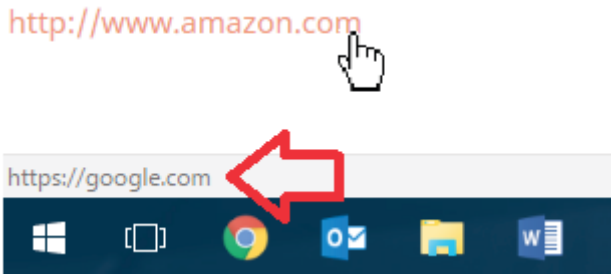
While many of the phishing emails you'll receive are clearly fakes littered with spelling and grammatical errors, obviously false email addresses, and nonsensical instructions, these attacks are becoming more sophisticated every day. Many are difficult to distinguish as fake. Here are a few techniques they use and how to spot them:

Fake links

Hyperlinks can look like they will lead you to a legitimate site, but they can actually go wherever the creator wants them to. For example, you would expect clicking this link: http://www.amazon.com would take you to Amazon, right? However, I've told the code powering it to direct the clicker to Google instead.

The text shown and the actual link destination don't have to match whatsoever. This is how scammers trick people into thinking they're going to something like their bank website when in fact they're going to that scammer's fake bank login page.

So how can you tell where a link will take you? By hovering your mouse cursor over the link without clicking, a bar will pop up in the lower left corner of your screen that shows where you will go when you click. Here's an example with that same Amazon-Google link trick:



Email address spoofing

Spoofing really just means faking, and it's the term for when scammers mask their sending address to make it look like the email is coming from someone else - a trusted organization, family member, or friend for instance to improve the chance that you'll click on their link.

Unfortunately there is really no easy way to determine when this is happening just by looking at the address. Best practice is to not click links in these emails unless you were expecting them, and contact the sender by phone or in person when in doubt.

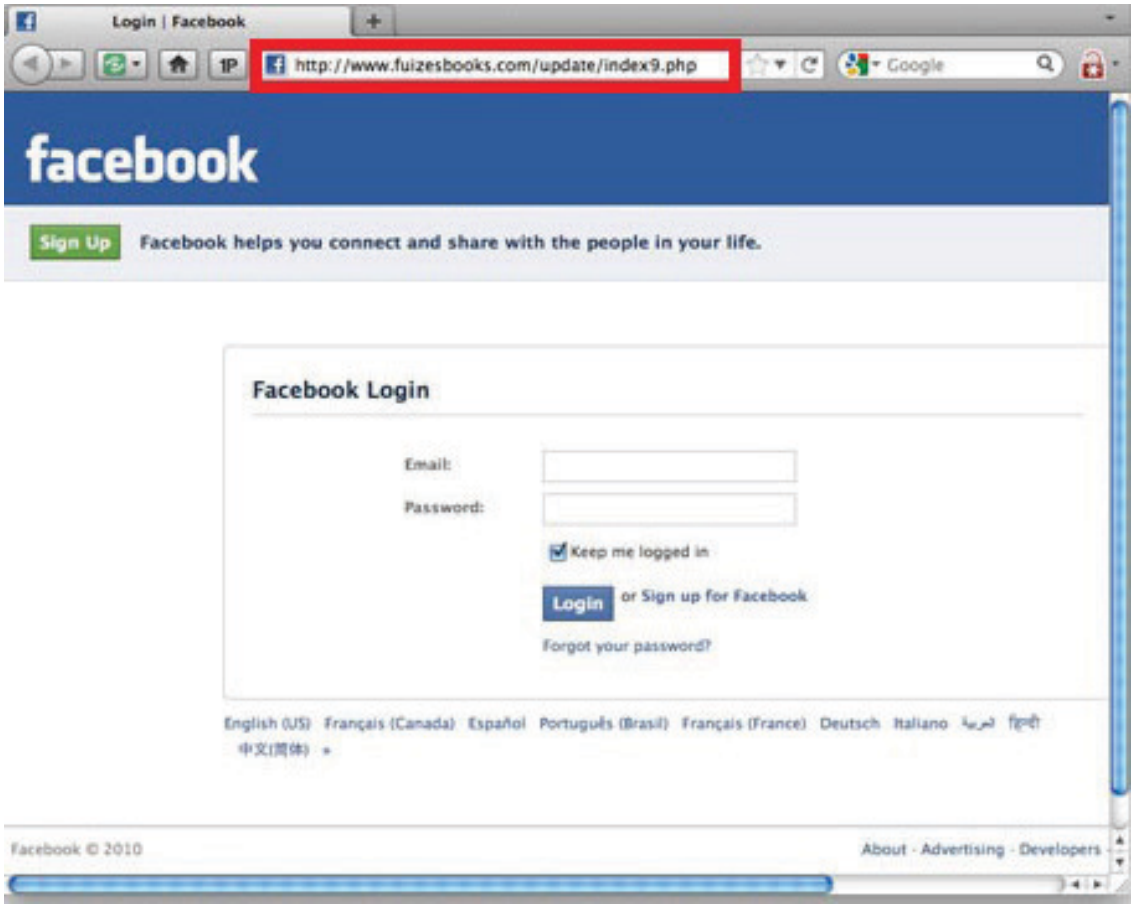
People whose email accounts have been hacked may also send out mass emails with bogus links.

Website dupes

Fake links in emails often lead to phony websites, clones of reputable sites that attackers hope are convincing enough to trick you.

It may look like you're on Facebook's login page, but you're about to send your credentials to a criminal! Always be aware of what you're clicking on, and what the page URL you're on looks like.

Many people won't take the time to notice where they're actually about to login:



To make the fake website issue worse, attackers can do what's called pharming. This method allows the criminal to redirect you to a malicious website from a reputable website. For example, you could type in "business.com" and if it's been overtaken by pharming, you'll be sent to "terrible-infected-website-that-will-steal-your-soul.com" instead.

To protect against getting duped this way, ensure you're checking the URLs of any website you need to enter personal or financial information into. Using an antivirus and/or content filtering program will also help prevent any issues by blocking the malicious website from loading at all.

To click or not to click?

> It's best to treat emails with links like emails with attachments. If you are expecting the email - say you just ordered a package from Amazon and receive an email with your tracking code - go for it. If the email is out of the ordinary, unexpected, asks you to confirm/enter financial or personal information, or looks "phishy" in any way, it's best to err on the side of caution.
>
> Businesses that handle financial and personal information have strict rules against ever asking you for information over email. You can always call to confirm the information from the email, or instead manually log into the website account in question without following the provided link.

How to handle a successful phishing attack

While these are steps we like, we recommend always checking with your dedicated IT person or company (if you have one) before doing anything yourself. They likely have a preferred method based on the company's needs and setup, and trying to handle something your own way may mess that up!

If your business has fallen victim, here are some steps you can take to minimize and reverse any damage:

- Engage the help of your IT support – if you don't have a full-time person or team, get in touch with a trusted service provider (but be aware you may have to pay emergency rates).
- Identify the source of the breach and which users were the cause. But don't shame or embarrass them! You want to encourage a culture of openness, especially around security. The damage is done, whether they try to hide it or not. The more information you can get from them to prevent issues in the future, the better. Ask why they clicked/entered their information, what they thought was convincing about the scam, and what happened before/during/after they were victimized.
- Alert your financial partners - let your business banks know what's going on and set up charge alerts if you haven't already. If you suspect your debit/credit cards may have been compromised, request new ones.
- Do clean up – attacks on businesses are often out for credentials and information they can use later. Have the team change the passwords of any accounts that use the same login information as the stolen one. Completely hanging all business passwords is even better.
- Turn it into a learning session – once everything is back to normal, it's a great time to up you and your team's security knowledge. An IT or security consultant/trainer could come in to conduct a team training. You can find tons of resources online to send to your team (like this one!) You can even use tools to conduct simulated phishing attacks to find and remediate the weak points in your company. Check out the next section for links to some of these resources.

Additional security training and resources

- The Business Guide to Cybersecurity (eBook)
- How to Create (and Remember!) Strong Passwords (Article)
- IronScales - Attack simulation, awareness training, real-time threat protection for your email accounts
- KnowBe4 – Security awareness training and simulated attacks
- PhishProof – Phishing simulations and reporting
- Phishd – Simulated phishing attacks, training, security audits, and reporting

Request your complimentary business security review

It's so important to know your business is protected from cybercriminals, phishing, malware, and other security threats. We'd love to help give you that peace of mind. Click the link above to schedule a security review with us - no pressure, no slimy sales pitches, just advice on how to keep your company protected!