Online Security Tips

Aug 4, 2020	KnowBe4 Human error. Conquered. **Scam of the Week: Sneaky "Service Desk" Scam** A new phishing attack is using a number of tactics to trick unsuspecting users into handing over their login credentials. The email claims you have unread emails due to your cloud storage being full. It then gives you options to resolve the issue. Clicking on either link sends you to a phony login page for your service provider. And any information on this page will be sent directly to the scammers. What makes this scam so sneaky? First, the phony log-in page not only looks official, but also functions like a real login page. Only passwords that meet real requirements are accepted. If an acceptable password is entered, you are redirected to the actual website of the service provider you just provided credentials for. Second, the email is sent from a no-reply address using the domain "servicedesk.com". Most of us are used to seeing emails from support desks, which makes this sender feel legitimate. Third, the email itself bypasses security filters that you may have in place by using a combination of factors that makes your email security filters think the link is secure. Don't be fooled! Remember these tips: • Phishing emails are often designed to create a sense of urgency. In this case, the idea that you're missing important emails. Think before you click, the bad guys rely on impulsive clicks. • Email security filters can only do so much to protect your sensitive information. Stay alert and help create a human firewall for your organization. • When an email asks you to log in to an account or online service, log in to your account through your browser and not by clicking the link in the email. That way, you can ensure you're logging into the real website and not a phony look-a-like. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
July 27, 2020	KnowBe4 Human error. Conquered. **Scam of the Week: Smishing for Access to Your Bank Account** Emails are a quick and easy way for cybercriminals to phish for your information—but it's not their only tool. Smishing, or SMS Phishing, is another way the bad guys try to trick you. Many of us are used to receiving legitimate promotions, reminders, and security notifications via text message. These messages—both real and fake—are brief and often include links, so it can be difficult to spot a smishing attempt. One recent example involves scammers posing as your local postal service while sending malicious text messages as part of their smishing attack. The message claims that you have a package waiting for pick up, but to see more information you must click the link in the text. If you click the link, you're taken to a phony verification page. Here, you're asked to enter your banking information in order to verify your identity. If you provide any information on this page, your data is sent directly to the cybercriminals—giving them full access to your bank account. Don't be fooled!

	Here's how to stay safe from this smishing attack: • Think before you click. Are you expecting a package? Is this how the postal service usually handles things? Consider anything out of the ordinary a red flag. • Never trust a link in an email or text message that you were not expecting. Instead of clicking the link, open your browser and type the official URL of the website you wish to visit. • Go old school. Pick up the phone and call your local post office. Be sure to call their official phone number—not the one that sent you the suspicious text message. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
July 17, 2020	 Scam of the Week: Not So Fast! Is Your Zoom Account Really Suspended? Whether you are commuting to an office or working from home, millions of employees rely on video conferencing apps like Zoom, to stay connected. If you were suddenly notified that your Zoom account had been suspended, how eager would you be to resolve the problem? Cybercriminals assume you'll be quick to respond. In fact, they hope you won't think twice about it. A recent phishing scam spoofs an email notification from Zoom. The email claims that your account has been suspended and that you are unable to make or join video calls until you click the "Activate Account" button included in the email. Once you've clicked the button, you are brought to a convincing Microsoft 365 look-a-like login page. If you enter your details on this page, this information will be sent directly to the scammers. The bad guys could use your login credentials to gain access to your organization's network and sensitive information. Keep you and your organization safe with these tips: • Never click on a link within an email that you weren't expecting. • Remember that email addresses can be spoofed. Even if the email appears to be from a familiar organization, it could be a phishing attempt. • When an email asks you to log in to an account or online service, log in to your account through your browser—not by clicking the link in the email. That way, you can ensure you're logging into the real website and not a phony look-a-like. Stop, Look, and Think. Don't be fooled. The KnowBe4 Security Team KnowBe4.com
July 14, 2020	 Scam of the Week: Exploiting the Coronavirus: A Sneaky Pandemic Relief Scam A new phishing email—seemingly sent from your local government funding agency—is offering phony relief grants to those in need.

	What makes this scam especially sneaky is that the bad guys use a Dropbox link to disguise their malicious attachment. Dropbox is a legitimate and commonly-used file sharing service. Therefore, the email security filters that your organization has in place may not consider the link as a red flag– increasing the chances of this email landing in your inbox. The phishing email urges you to click a Dropbox link so you can download a file that supposedly contains information about your relief grant payment. The link even includes an expiration date for an added sense of urgency. If you click the link, then, download and open the phony file, you're taken to a look-a-like Microsoft 365 login page. If you enter any information on this page it will be sent directly to the scammers. Remember these tips: • Never click a link or download an attachment from an email that you weren't expecting. Even if the sender appears to be a legitimate organization, the email address could be spoofed. • Be cautious of unexpected deadlines. Scammers often create a sense of urgency to spark impulsive clicks. • Get confirmation before clicking a Dropbox link. If you feel the file could be a legitimate resource for your organization, reach out to the sender another way—like by phone—instead of trusting the email. Stop, Look, and Think. Don't be fooled. The KnowBe4 Security Team KnowBe4.com
July 9, 2020	KnowBe4 Human error. Conquered. KnowBe4 Security Tips - CRA and Tax Scams Every year, the bad guys take advantage of innocent taxpayers, like you, who are patiently waiting on their tax return. Last year, the CRA noticed a significant increase in phishing attempts to steal money or tax data, therefore you must be on high alert. How it Happens: Tax Scams and Malicious Activity The bad guys have a number of tax-related tricks up their sleeves when it comes to stealing your money and/or sensitive information. Here are a few examples of sophisticated tax scams that have been found in the wild: • Scammers send emails posing as tax service companies by spoofing emails and using stolen logos. Once you respond to the email with personal data or tax information, they can pocket your hard-earned money. • Similar to the scam above, the bad guys send look-alike emails containing hyperlinks that lead you to malicious websites or fake PDF attachments that download malware or viruses to your computer. • Tax scams aren't limited to emails! Be on the look out for callers posing as CRA representatives claiming you owe money that must be paid immediately. The callers typically threaten arrests, deportation, or suspension of business or driver's license. Keep in mind, these are only a few examples and these scam artists are constantly coming up with new ways to fool you. How Do I Know it's a Scam? Always remember the following during tax season, and all year long: • The CRA will always mail a bill before calling you about taxes owed. • The CRA will never ask for credit or debit card numbers over the phone. • The CRA will never immediately threaten to arrest you for not paying taxes owed. • The CRA will always offer the opportunity to question or appeal the amount owed before demanding your payment.

	• The CRA does not use emails or text messages to discuss personal tax matters, such as taxes owed or tax refunds. Only share sensitive data over email when there is no other alternative and you're certain the recipient is valid. Stop Look Think - Don't be fooled The KnowBe4 Security Team KnowBe4.com
July 6, 2020	 Scam of the Week: Survey Says… It's a Scam Some retailers use online surveys to learn more about their customers. Completed surveys are often rewarded with small consolations, like a coupon. Sounds fun, right? The bad guys sure think so! Scammers are posing as well-known brands and sending emails that advertise extravagant rewards, like a new iPhone, for just a few minutes of your time. Typically, the survey website displays a message claiming that there are only a small number of rewards remaining—this creates a sense of urgency to complete the survey. Usually, at the end of the survey, you're told that you have won the prize and all that you have to do is pay for delivery. Of course, you didn't actually win anything. The fake prize and request for your shipping details are just an excuse to gather your name, address, and payment information. Don't let the scammers win! Follow these tips when you are answering retailer surveys: • Always question a sense of urgency. Real companies want real results. If a survey is urging you to hurry, it's because they want to get to the part where you hand over your personal information. • Legitimate retail surveys clearly outline the rules from the very beginning. If you're suddenly asked for payment or other unexpected information, it's a scam. • If it sounds too good to be true, it is! As lovely as it would be, no one hands out free iPhones (or other extravagant rewards) over the internet. Stop, Look, and Think. Don't be fooled. The KnowBe4 Security Team KnowBe4.com
June 29, 2020	 Scam of the Week: Phony LogMeIn Security Updates LogMeIn is a popular remote access tool used by IT professionals to gain entry to their employees' machines. These tools are especially popular right now with so many people working remotely. Unfortunately, with popularity, comes risk. Cybercriminals are impersonating LogMeIn in a new phishing attack. The phishing email claims that you need to click a link in the email to download an "urgent security update". If you click this link, it takes you to a phony login page for LogMeIn. If you enter your credentials on this look-alike page, the information will be sent straight to the bad guys. If you fall for this trick, you could give attackers access to countless machines within your organization's network. Stay safe by following these tips: • Never click on a link within an email that you weren't expecting.

	• If you are prompted to update any software on your work device, reach out to your administrator or IT department so they can check that the update is legitimate and safe. • When an email asks you to log in to an account or online service, log in to your account through your browser–not by clicking the link in the email. That way, you can ensure you're logging into the real website and not a phony look-alike. Stop, Look, and Think. Don't be fooled. The KnowBe4 Security Team KnowBe4.com
June 23, 2020	KnowBe4 Human error. Conquered. KnowBe4 Security Tips - Booking a Vacation Rental? "Getaway" From These Scams! Getting ready for a vacation? If you plan to use a popular vacation rental website or application (app), such as, AirBnB, HomeAway, or VRBO to find your next getaway, beware. Cybercriminals are using these services to trick you and steal your money. How Does It Work? The scammers often post completely fake rental listings using images they find on the internet, or they steal pictures and property details from legitimate rental listings to create their own listing with the scammer's contact information. When someone inquires about a fake listing, the scammer will request a security deposit or a portion of the full rental price as a down payment. Once the scammer has your money, they'll cancel the reservation at the last minute, or you will arrive at your vacation home to find that the property is already booked, or that the property doesn't even exist. How Do I Know It's a Scam? Don't let the scammers ruin your vacation. Remember the following tips when you're booking your next vacation rental online: • Book official. Only use reputable websites that offer protection against fraud and have a secure payment portal. • Make sure that the property exists. Search for the property on Google Maps or another mapping service. If you know someone in the area that you will be visiting, ask them to check out the property for you. Scammers might use an address that does not exist, or use the address of a random company, vacant building, or parking lot. • Research the rental listing. Search online for the property owner's name and address, and look for images of the property, before you make a deposit. If you find multiple listings with different contact information, reconsider booking the property. • Read the reviews. If a property has multiple negative reviews, or doesn't have any reviews, consider a different property. • Only make payments through the official website for the rental listing. Scammers often try to get you to pay with a check, get you to wire them money directly, or use services like MoneyGram or Western Union to make a payment. Stop Look Think - Don't be fooled The KnowBe4 Security Team KnowBe4.com
June 22, 2020	KnowBe4 Human error. Conquered. **Scam of the Week: SpaceX YouTube Scam**

	Scammers recently hijacked three YouTube channels and used them to collect nearly $150,000 in cryptocurrency. They used these stolen channels to impersonate the official SpaceX YouTube channel. The hijackers played fake livestream interviews with Elon Musk, founder and CEO of SpaceX, while promoting bogus cryptocurrency giveaways. These giveaways are based on an old-school scamming tactic in which cybercriminals ask for a small payment while promising a large payout for the so-called investment. This scam was successful for two main reasons: First, using existing YouTube channels gave the cybercriminals a large, trusting audience of subscribers. Second, the scammer's "investment offer" appeared to be coming from the well-known, tech-savvy billionaire, Elon Musk–rather than from a random stranger–so it seemed to be more legitimate. Here's what we can learn from this scam: • If something seems too good to be true–like an unbelievable investment opportunity–it probably is! Question everything. • Whether it's a phony website, a disguised email address, or a hijacked YouTube channel, anyone and anything can be spoofed. • Experts speculate that the scammers gained access to these YouTube channels through a data breach of a different website. This is a great example of why you must use a different password for every login. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
June 1, 2020	KnowBe4 Human error. Conquered. ## Scam of the Week: Exploiting the Coronavirus: Malicious Zoom Installer Whether you're working from home or trying to stay in touch with loved ones, video conferencing apps like Zoom are becoming the new normal. Cybercriminals have exploited this type of application before, but their latest scam may be the trickiest yet. Scammers are sending out phishing emails with links to download the latest version of Zoom. When clicked, the link takes you to a third-party website–not the official Zoom site–to download an installer. If you download and run the file, the program truly does install Zoom. The trick is, the installer also places a remote access trojan (RAT) on to your computer. This RAT gives cybercriminals the ability to observe everything you do on your machine. This includes keylogging (saving what you type), recording video calls, and taking screenshots–all of which can be used to steal your sensitive information. Don't fall victim to this scam! Remember the following: • If an email directs you to install or update an application, do not click on the link in the email. Instead, go directly to the official website through your browser. This ensures you are accessing the real page and keeping your credentials safe. • When using a work device, reach out to your IT department before installing any software. They can check that the application is legitimate and safe.

	Stop, Look, and Think. *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
May 25, 2020	 **Scam of the Week: Exploiting the Coronavirus: Phony COVID-19 Tracking** Countries around the world are developing COVID-19 tracking applications for mobile devices. These apps use digital tracking to help identify and notify users who have been in contact with someone diagnosed with the virus. Only a handful of countries have released this kind of app to the public, but cybercriminals are already using them as inspiration for scams. The bad guys are sending phishing emails and smishing attacks (phishing via text messages) claiming that you have been in contact with someone diagnosed with Coronavirus. The message insists that you get tested and it includes a link that supposedly leads to a website where you can sign up for more information. The truth is, the link takes you to a malicious website that is designed to steal any information you enter and deliver it to the bad guys. Don't be fooled! Remember these tips: • Never click on a link from an email or text message that you weren't expecting–even if it appears to be from a legitimate organization. • Think before you click. The scammers are expecting an impulsive click. • Stay up-to-date on local regulations and containment efforts through official government websites and trusted news sources. *Stop, Look, and Think.* ***Don't be fooled.*** ***The KnowBe4 Security Team*** ***KnowBe4.com***
May19, 2020	 **Scam of the Week: Exploiting the Coronavirus: From Unemployed to Money Mule** Due to the Coronavirus crisis, unemployment numbers have skyrocketed. As usual, the bad guys are quick to take advantage of these hard times and are sending out phony work-from-home opportunities. Typically, these phishing emails contain grammar mistakes and offer minimal details about the hiring company and the job requirements. But the scammers still manage to grab your attention because the job opportunity includes a great paycheck. Once accepted, these scammers ease the victim into their new "job", by asking them to complete basic errands, but eventually they're given the task of transferring funds from one account to another. Typically, these are stolen funds

	and the unsuspecting "employee" is being used as a money mule. Even though these victims are unaware of the crime they are committing, they can still face hefty fines and prison time. Remember these tips and share them with your friends and family who may be looking for work: • Be wary of emails with spelling or grammatical errors. • Never trust unusual requests or job offers. If something doesn't feel right, it probably isn't. • If you feel you have been solicited to be a money mule, contact your local authorities or report the situation to the appropriate federal agency. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
May 11 2020	 **Scam of the Week: Exploiting the Coronavirus: Netflix is More Popular Than Ever - Especially with Cybercriminals** Long before the COVID-19 pandemic, bad guys were spoofing Netflix emails in an attempt to collect your sensitive information. With more and more people looking for at-home entertainment, Netflix has gained over 15 million new subscribers. Cybercriminals are happily taking advantage of this larger audience! Netflix themed phishing attacks can vary from phony email alerts accusing you of non-payment to offering you free streaming access during the pandemic. Both of these strategies include a link that takes you to a fake Netflix page designed to gather your information and deliver it to the bad guys. Use the following tips to stay safe: • These types of scams aren't limited to Netflix. Other streaming services like Disney+ and Spotify are also being spoofed. Remember that if something seems too good to be true, it probably is. • Never click on a link that you weren't expecting. Even if it appears to be from a company or service you recognize. • When an email asks you to log in to an account or online service, log in to your account through your browser - not by clicking the link in the email. This way, you can ensure you're logging into the real website and not a phony look-alike. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*

May 11 2020	 KnowBe4 Security Tips - Don't Trust Pop-ups If you're known to dabble in a little online browsing, odds are you've encountered a pop-up once or twice. There are times when a user may think, "Wow, that's a great deal!" and click on a pop-up. To those users: put down the mouse. Why? That pop-up could be malicious or dangerous. There used to be a time when malicious pop-ups were only on questionable sites, but those days are gone. Hackers are smart and develop ways to inject malicious malware into pop-ups and online advertisements - even on the most trusted sites. One of the most common attacks we see occurs when you visit a site and a pop-up appears that says, "Your computer is infected! Download our antivirus now!" If you click on this, a bogus virus scan will start. After the "scan" completes, you'll be asked to pay for a full-version of the software or to call a helpline to connect with a support representative. Spoiler alert: The software is not real and the fake support representative will take control of your computer to try and "fix" the issue, but end up causing more damage. **How to prevent** Although hackers are smart, you can be smarter. Here are some tips to protect yourself from these types of attacks: • Avoid clicking on pop-ups. • Update your operating system regularly - don't postpone or snooze updates! • Use web-filtering software to warn you before accessing potentially harmful sites. Remember, these attacks are only successful if we fall for them. Stay alert and be cautious! Stop Look Think **- Don't be fooled** ***The KnowBe4 Security Team*** ***KnowBe4.com***
May 4 2020	 ## Scam of the Week: Exploiting the Coronavirus: Smishing Violation! Governments across the globe have created restrictions to help reduce the spread of Coronavirus. These regulations change often and vary by country, region, and city. So knowing exactly what is expected of you can be a challenge. It's no surprise that the bad guys are taking advantage of this confusion! Cybercriminals are using text messaging, or short message service (SMS), to pose as a government agency. The message says you have been seen leaving your home multiple times and as a result you are being fined. They urge you to click on their official-looking link to pay this "fine" online. If you click the link, you'll be taken to a payment page where you can give your credit card details directly to the bad guys!

	This tactic is known as “Smishing” (SMS Phishing). Smishing can be even more convincing than email phishing because criminals know how to spoof their phone number to appear as though they're calling from an official source. Be careful! Here’s how to stay safe from this smishing attack: • Think before you click. The bad guys want to get under your skin. Not only does this message accuse you of ignoring regulations, but it also claims you have to pay a fine! Don’t give in to this tactic. • Never trust a link in an email or text message that you were not expecting. Instead of clicking the unexpected link, open your browser and type in the official URL of the website you wish to visit. • Stay informed during this confusing time by following local news, government websites, and other trusted sources. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
Apr 17 2020	KnowBe4 Human error. Conquered. **Scam of the Week: Exploiting the Coronavirus: Re-opening your organization? The bad guys have a plan!** Recently, some countries have chosen to lift restrictions that were originally put in place to control the spread of COVID-19. Beware! The bad guys are already taking advantage of this news. They have crafted a well-written phishing email that appears to come from the VP of Operations in your organization. The message claims that your organization has a plan for reopening, and it instructs you to click on a link to see this plan. Clicking the link opens what appears to be a login page for Office365, but don’t be fooled! If you enter your username and password on this page, you would actually send your sensitive credentials directly to the bad guys. Here’s how to protect yourself from this clever attack: • Never click on a link or an attachment that you weren’t expecting. Even if it appears to be from someone in your own organization, the sender’s email address could be spoofed. When in doubt, reach out to the sender by phone to confirm the legitimacy of the email before clicking. • When an email asks you to log in to an account, do not click the link in the email. Instead, go directly to the website through your browser. This ensures you are accessing the real page and keeping your credentials safe. • This attack tries to exploit the restlessness and uncertainty of life in quarantine. Don’t let the bad guys toy with your emotions. Think before you click! ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*

Apr 20 2020	 **Scam of the Week - Exploiting the Coronavirus: "PANDEMIC IS WITHIN, BEWARE!"** During this storm of COVID-19 phishing scams, the bad guys love posing as your trusted Human Resources department. One recent HR scam started with an overdramatic subject line: "COVID-19 PANDEMIC IS WITHIN, BEWARE! WARNING!!!" In a mess of run-on sentences, the email claims that some of your co-workers have tested positive for Coronavirus. Keeping with the HR theme, they ask that you do not discriminate against these people and they suggest that "everyone should rather cease panic". The email does not identify anyone by name, but asks you to download an attached photo of the infected employees. This attack targets your natural curiosity. *Who could it be? Wasn't Bill coughing last week? I just* have *to know!* If you were to download the attachment, you would find that it is actually a piece of malicious software designed to quietly steal data through your organization's network. Don't be fooled! Remember these tips: • Watch for sensational words like "BEWARE" and "WARNING!!!" The bad guys want you to panic. • Be wary of emails with spelling or grammatical errors, especially when it supposedly came from a reputable source. • When questioning the legitimacy of an email sent from someone in your company, give them a call! One quick call could save your organization from a potential data breach. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
April 14 2020	 **Scam of the Week - Exploiting the Coronavirus: Is the CDC Closing Your Facility?** As the COVID-19 pandemic rages on, the bad guys find increasingly creative ways to weaken your defenses. The newest phishing trend is an email that appears to be from the CDC (Centers for Disease Control and Prevention). The email has an intense subject line: "NOTICE OF CLOSING YOUR FACILITY AND DISINFECT NG THE AREA - BY NCDC WH 20982 COV-19 Due To Recent Corona Virus COVID-19 Pandemic."

	You're instructed to download an attachment which is supposedly a letter from the CDC claiming that they will close your facility. If you download the file, you'd find that it is actually a malicious program designed to gain access to your company's sensitive information. Don't be tricked! How to beat the bad guys: • Think before you click. These malicious actors are playing with your emotions and this threat relies on panicked clicking. • Never click a link or download an attachment from an email you weren't expecting. Remember, even if the sender appears to be a legitimate organization, the email address could be spoofed. • If you receive a suspicious email that claims to be from an official organization such as the CDC or WHO (World Health Organization), report the email to the official organization through their website. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
April 6, 2020	KnowBe4 Human error. Conquered. **Scam of the Week - Exploiting the Coronavirus: Fear of Infection** The newest Coronavirus-themed phishing attack may be the most ruthless yet. The cybercriminals are sending emails that appear to be from a hospital and warn that you have been exposed to the virus through contact with a colleague, friend, or family member. Attached to the email is a "pre-filled" form to download and take with you to the hospital. Don't be fooled. The attachment is actually a sophisticated piece of malware. This threat relies on panic and fear to bypass rational thinking. Don't give in! Remember to stay vigilant: • Think before you click. The bad guys rely on impulsive clicking. • Never download an attachment from an email you weren't expecting. • Even if the sender appears to be from a familiar organization, the email address could be spoofed. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
March 27, 2020	KnowBe4 Human error. Conquered.

Scam of the Week: Working From Home? Don't Fall for This "Phony" Call

The Coronavirus Disease 2019 (COVID-19) pandemic has caused a massive shift in the number of employees who are working remotely. From a cybercriminal's perspective, this is a perfect opportunity for their social engineering scams.

One scam involves cybercriminals calling you and posing as support personnel from the companies or services that your organization may be using to allow you to work remotely. Typically, the caller will try to gain your trust by stating your job title, email address, and any other information that they may have found online (or on your LinkedIn profile). Then, the caller claims that they will send you an email that includes a link that you need to click for important information. Don't fall for this scam!

Remember the following to help protect yourself from these types of scams:

- Never provide your personal information or work information over the phone unless you're the one who initiated the call.
- Scammers can spoof any number they'd like. Therefore, even if a call looks like it's coming from a legitimate source, it could be a scam.
- If you receive this type of call, hang up the phone immediately and notify the appropriate team in your organization.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com

March 13, 2020

KnowBe4
Human error. Conquered.

Scam of the Week: Exploiting the Coronavirus: Watch out for These Scams!

Look out! The bad guys are preying on your fear and sending all sorts of scams related to the Coronavirus (COVID-19).

Below are some examples of the types of scams you should be on the lookout for:

1. Emails that appear to be from organizations such as the CDC (Centers for Disease Control), or the WHO (World Health Organization). The scammers have crafted emails that appear to come from these sources, but they actually contain malicious phishing links or dangerous attachments.
2. Emails that ask for charity donations for studies, doctors, or victims that have been affected by the COVD-19 Coronavirus. Scammers often create fake charity emails after global phenomenons occur, like natural disasters, or health scares like the COVID-19.
3. Emails that claim to have a "new" or "updated" list of cases of Coronavirus in your area. These emails could contain dangerous links and information designed to scare you into clicking on the link.

Remain cautious! And always remember the following to protect yourself from scams like this:

	• Never click on links or download attachments from an email that you weren't expecting. • If you receive a suspicious email that appears to come from an official organization such as the WHO or CDC, report the email to the official organization through their website. • If you want to make a charity donation, go to the charity website of your choice to submit your payment. Type the charity's web address in your browser instead of clicking on any links in emails, or other messages. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
March 8, 2020	KnowBe4 Human error. Conquered. **KnowBe4 Security Tips - Social Engineering Red Flags #4: Links/Attachments** The prevalence of phishing scams is at an all-time high. You are the key to preventing a cyberattack, it is important to question the legitimacy of every email you receive. Below is a list of questions to ask yourself about any **links** or **attachments** on the email that may help you realize that you are being phished. **Are there hyperlinks in the email?** • Hover over any links and check the link address. Does it match the website for the sender exactly? • Did you receive a blank email with long hyperlinks and no further information or context? • Does the email contain a hyperlink that has a misspelling of a well-known website? (Such as Micorsoft) • Is the sender's email from a suspicious external domain? (like micorsoft-support.com rather than microsoft.com) **What about attachments?** • Did the sender include an email attachment that you were not expecting or that makes no sense in relation to the email's context? • Does the sender ordinarily send you these types of attachments? • Did the sender send an email with a possibly dangerous file type? Files with a .TXT extension are *typically* safe, but beware, files can be disguised with a different type of file extension. If you notice anything about the email that alarms you, do not click links, open attachments, or reply. You are the last line of defense to prevent cyber criminals from succeeding and making you or your company susceptible. **Stop Look Think** - Don't be fooled *The KnowBe4 Security Team* *KnowBe4.com*

March 6, 2020	 ## Scam of the Week: Convincing Smishing Scam from a Popular Mobile Carrier Not only do internet criminals phish your email inbox, they also send text messages to try their malicious tricks. Using text messages, or short message service (SMS), for phishing attempts is known as “Smishing”. Recently, smishing scammers have been sending text messages that appear to come from the popular cell phone service provider, Verizon. The text message is designed to look like a security alert. It warns you to click the link and validate your account before your account access is disabled. If you fall for this alert and click on the link, you’re brought to a very convincing fake website that looks identical to Verizon’s login page. You’re instructed to sign in to your account to “validate your account security”, but if you mistakenly enter your credentials here, the attackers will have your login information and be able to take over your account. Remember the tips below to protect yourself from smishing scams: • Links sent through text messages are usually shortened. Therefore, you can’t see where the link will actually take you. If your mobile device allows it, before clicking the link, hold your finger down to see the full web address of where the link will take you. • Always log in to your online accounts through your phone’s browser or through the mobile application you’ve installed on your phone, instead of clicking an unexpected link. • Never use the same password for multiple accounts. If you did fall for a scam such as this you may not even realize it happened, but the attackers would be able to break into all of the accounts where you use the same password. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
March 2, 2020	 ## Scam of the Week: Watch out for Malicious Apps in Your App Store Google recently removed several applications (apps) from their Google Play store because they contained a strain of “clicker” malware that can view your sensitive data and even make in-app purchases on your behalf. Even though they have now removed these apps there could still be more they don’t know about. This is *not* the first time that applications with “clicker” malware have been removed from official Android and Apple app stores, and it will not be the last. Ensuring the security of mobile applications is an ongoing challenge. Consider the following before downloading any application:

	• Do your research: Read app reviews, but make sure they're not fake or staged! Be wary of applications that don't have any reviews. • Avoid applications that have a low number of downloads. • Look for strange context or spelling errors in the application's description. • Consider investing in cybersecurity protection for your mobile device. When in doubt, avoid downloading questionable applications, and look for a safer alternative. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
February 24, 2020	KnowBe4 Human error. Conquered. **Scam of the Week: Watch Out for This Clever New Credit Card Phishing Scam** Look out! The bad guys are sending a new, attention-grabbing phishing email and they're targeting the customers of major credit card companies. Here's how it works: The email appears to come from one of two well-known credit card companies, either American Express or Chase. The email includes a list of credit card transactions, and you're asked to confirm or deny whether the transactions are valid. If you click the "No, I do not recognize the transactions" link, you're brought to a fake login page that looks very similar to the credit card company's actual login page. Don't fall for this trick! If you submit your login details, your information is immediately sent to the scammers and your account and your identity will be at risk. Remember the following to help protect yourself from these types of scams: • Do not trust the links in an email that you weren't expecting. • When you receive an email asking you to log in to an account or online service that you use, log in to your account through your browser–not through links in the email. This way, you can ensure you're logging into the real website and not a phony look-alike. • Do not reuse passwords. If you use the same password for multiple accounts and one gets hacked, they're all at risk of being hacked. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
February 14, 2020	KnowBe4 Human error. Conquered.

Scam of the Week: Another SMS Scam - PayPal Edition

Cyber scammers don't limit their phishing attacks to your email inbox, they love texting your mobile device too! Their current text, or Short Message Service (SMS), scam uses PayPal as the bait.

The text message claims to be from PayPal, and it states that there has been unusual activity detected on your account. If you click on the link in the text, you're taken to a phishing site that looks almost identical to PayPal's login page. You are prompted to enter your email address and then your password. Once you've gotten this far, you're asked to enter your mother's maiden name, your home address, and your financial details. Do not enter any of your information! If you do, your details are immediately sent to the attackers, and your account and your identity are at risk.

Always remember the following to help protect yourself:

- Never click on links in a text message or an email that you weren't expecting.
- When you receive a message asking you to log in to an account or online service, navigate to the login page from your phone's browser or use the service's official mobile application. This way, you can ensure you're logging in to the real website.
- Do not reuse passwords. If you use the same password for multiple accounts and one gets hacked, they're all at risk of being hacked.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com

February 10, 2020

KnowBe4
Human error. Conquered.

KnowBe4 Security Tips - How Secure is Your Mobile Device?

Most of us have a smartphone, but how many of us really think about the security threats faced by these mobile devices? Mobile devices are vulnerable to many different types of threats. The bad guys are increasing attacks on mobile devices and targeting your phone using malicious applications. Using these methods, they can steal personal and business information without you having any idea what's going on.

Even if you've downloaded a security or antivirus application, securing your smartphone goes beyond these services. Improving your mobile security practices is your best defense against the privacy and security issues associated with your mobile device.

How can I improve my mobile security practices?
Always remember these best practices to minimize the risk of exploits to your mobile devices:

1. **Ensure your phone's operating system is always up to date.** Operating systems are often updated in order to fix security flaws. Many malicious threats are caused by security flaws that remain unfixed due to an out of date operating system.
2. **Watch out for malicious apps in your app store.** Official app stores regularly remove applications containing malware, but sometimes these dangerous apps slip past and can be downloaded by

	unsuspecting users. Do your research, read reviews and pay attention to the number of downloads it has. Never download applications from sources other than official app stores. 3. **Ensure applications are not asking for access to things on your phone that are irrelevant to their function.** Applications usually ask for a list of permissions to files, folders, other applications, and data before they're downloaded. Don't blindly approve these permissions. If the permission requests seem unnecessary, look for an alternative application in your app store. 4. **No password or weak password protection.** Many people still don't use a password to lock their phone. If your device is lost or stolen, thieves will have easy access to all of the information stored on your phone. 5. **Be careful with public WiFi.** The bad guys use technology that lets them see what you're doing. Avoid logging in to your online services or performing any sensitive transactions (such as banking) over public WiFi. **Stop Look Think** - Don't be fooled *The KnowBe4 Security Team* *KnowBe4.com*
February 7, 2020	 ## Scam of the Week: Coronavirus Phishing Attacks The global threat of the coronavirus has everyone's attention, and the cybercriminals are already taking advantage of it. The bad guys are using the coronavirus as clickbait so they can spread malware and steal your personal information. They've crafted their phishing emails to look like they're coming from health officials such as doctors or national agencies, such as the Center for Disease Control and Prevention. Some of these emails suggest clicking a link to view information about "new coronavirus cases around your city". Other emails suggest downloading the attached PDF file to "learn about safety measures you can take against spreading the virus". Don't fall for it! If you click the phishing link, you're brought to a webpage that is designed to steal your personal information. If you download the PDF file, your computer will be infected with malware. Always remember: Never click on a link or download an attachment that you weren't expecting. Because of the alarming subject matter, the bad guys expect you to click or download without thinking. STAY ALERT! Don't be a victim. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
January 31, 2020	 ## Scam of the Week: Goodbye Windows 7, Hello Social Engineering Scams

	Recently, Microsoft announced they will no longer be supporting their Windows 7 operating system. This means there will be no further updates to Windows 7. The bad guys are using this situation to their advantage. They will randomly contact you by phone, emails, or pop-ups and try to convince you to pay yearly fees, or they'll insist that they need remote access to your computer so they can install "necessary" software. You'll lose your money if you mistakenly pay the fake fees, but if you grant the scammers access to your computer, your personal information and identity are at risk. Follow the tips below to help protect yourself from these types of scams: • **Microsoft support does not call customers.** If anyone calls you and claims that they are from Microsoft, this is a big red flag. Hang up the phone and ignore the request. If you want to speak with a legitimate customer support agent, go to Microsoft's website and find the company's customer support phone number. • **If a computer pop-up urgently claims that your computer needs an update to it's version of Windows 7...don't fall for it!** The bad guys add flashy pop-ups to websites to trick you into thinking your computer is at risk. Do not click on the pop-up or call any numbers that are listed. This is a scam! • **Do not share your credit or debit card information with anyone that calls you.** Never use a debit card to make online purchases, and only give someone your credit card data when you have initiated the phone call and you're sure the number is valid.
January 27, 2020	KnowBe4 Human error. Conquered. ## Scam of the Week: Cybercriminals Are Using Microsoft's Sway Application in Phishing Scams Most business environments trust the Microsoft brand and the bad guys often use this to their advantage. Now, they've figured out how they can use Microsoft's Sway application to steal your login details. Sway is used to create online presentations that are hosted on Microsoft-owned domains that you can share with anyone by sending a link. The phishing attack typically starts with an email that is disguised as a "New Fax Received" or "New Voicemail" notification. You're instructed to click a link in the email to view the message. If you click the link you're brought to a fake Microsoft login page that looks just like the real thing. Even the web address looks legitimate! That's because the login page is actually a presentation that was created with the Sway application. If you mistakenly enter your login details here, the criminals will steal this information and your account will be at risk. Remember the following to protect yourself from these types of attacks: • Never click on a link or an attachment that you weren't expecting. Even if it appears to be from a person of an organization that you're familiar with, the sender's email address could be spoofed. • Whenever you need to log in to an account or online service that you use, always navigate to the login page yourself using your browser, rather than clicking on links in an email. • Get familiar with the format of your fax and voicemail notification emails. If you're ever in doubt, contact the proper department in your organization before you click on any links or download attachments. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*

January 17, 2020	KnowBe4 Human error. Conquered. **Scam of the Week: Watch Out for "Free Gift" Scams** Watch out! Cybercriminals are posing as a mail carrier company that claims to have a "free gift" waiting for you. They start by sending a shipment notification email. The email includes a tracking code and other details about your package. If you click on the link in the email and enter your tracking code into this webpage, you're told that the package has arrived in your country but you must pay a very small delivery fee before you can claim it. If you fall for this offer and enter your payment details, your financial information is stolen and your "free gift" is never mentioned again. Here are a few reminders to help protect yourself from scams like this: • *Beware of free gifts.* If it sounds too good to be true, it probably is. Delete suspicious emails or follow the reporting procedures put in place by your organization. • *Be cautious of courier emails.* Delivery notification emails are often used in phishing attacks. Even if the email appears to be from a familiar organization, reach out to the sender directly (by phone) to get a trustworthy tracking number. • *"HTTPS" does not equal "secure".* These days, many cybercriminals are using "HTTPS" websites for their scams because most people look for a padlock in the address bar. However, the padlock does not guarantee that you're on a legitimate website, it only means that you're on a website that has obtained an HTTPS certificate. • *Don't click.* Never click on links or download attachments from emails you weren't expecting–even if it appears to be from a legitimate organization. ***Stop, Look, and Think.*** *Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*
January 17, 2020	central 1 Advisory: Intercepted e-Transfers We have detected a recent spike in an attack vector called "intercepted e-Transfers". What is an Intercepted e-Transfer you wonder? This can occur when you send an e-Transfer to someone you know. Criminals seize the opportunity to deposit the funds to a mule account before the intended recipient has the chance. The interception is not caused by a vulnerability in your online banking account or the *Interac* e-Transfer service, but rather because the recipient's email account was accessed by a criminal. Once in that account, criminals can "see" the notification from *Interac* and use the deposit link to redirect funds into a different account by answering the security question.

	Here are some tips to help you protect yourself: ▪ Do not communicate the answer to the security question via email. Call and/or text the recipient with the password. ▪ Select a question and answer that is not easy for a third party to guess. If the notification is intercepted, it will be harder for a criminal to answer and steal the funds. ▪ Be cautious not to click on any phishing links and ensure that they are only transacting with trusted websites, vendors and people. ▪ Immediately notify your financial institution if they sense anything suspicious about your transaction. ▪ Register for Auto Deposit. This will make sending money on the e-Transfer service more secure.
January 13, 2020	KnowBe4 Human error. Conquered. **Scam of the Week: Post-Holiday Shopping Scam** The holiday season has come and gone, but the bad guys are here to stay. Scammers are still using holiday shopping deals to lure you in. They're posing as popular retailers and sending dangerous emails and text messages that tell you to claim the reward points that you've supposedly earned with your holiday purchases. The bad guys use logos and company colors to make the emails and text messages look legitimate. Don't fall for it! If you click the phishing links in these emails or text messages, you are actually downloading malware to your computer or phone. This malware allows the criminals to gain access to your device; therefore, leaving your personal information at risk. Always remember: Never click on a link that you weren't expecting. If you receive an email from a retailer or service that you use, log in to your account through your browser (not through links in the email) to make sure it's valid. ***Stop, Look, and Think**. Don't be fooled.* *The KnowBe4 Security Team* *KnowBe4.com*