Online Security Tips

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	KnowBe4 Human error. Conquered. ## 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	

	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*