



## Resources to Protect Your Children, Your Parents and Yourself from Scammers and On-Line Criminals

### KEY TAKEAWAYS FROM THE PRESENTATION

- ✓ Please Think Before You Click
- ✓ Create Strong Passwords no shorter the 12 characters longer is always better
- ✓ Do Not Share Your Information Until You Confirmed the Source
- ✓ Automate Your Security Software Updates and Your Software Updates
- ✓ Back up your data remember the **3-2-1**
  - The rule is: Keep at least three (3) copies of your data and store two (2) backup copies on different storage media, with one (1) of them located offsite.
  - Secure your backups. Make sure they are not connected to the computers and networks they are backing up.
- ✓ Do not answer calls from someone you do not know; let it go to voice mail.
- ✓ Please, if you answer the phone and it is a Scam call, "DO NOT HANG ON, HANG UP."
- ✓ Never let a person who called you to pressure you in giving them your personal information or money.
  - Pause and use caution if you are being pressured for information immediately.
  - Please just hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request.
- ✓ Remember, you do not need to be a techie or a cybersecurity professional to protect yourself and your family.
  - You just need to be aware on how the scammers do their dirty work and where to go for information and help.
- ✓ If you have a voice mail account with your phone service, be sure to set a password for it.
  - Some voicemail services are preset to allow access if you call in from your own phone number.
  - The scammer/hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.
- ✓ Talk to your phone company about call blocking tools and check into apps that you can download to your mobile device.
  - The FCC allows phone companies to block robocalls by default based on reasonable analytics.
  - More information about robocall blocking is available at [fcc.gov/robocalls](http://fcc.gov/robocalls).
- ✓ Remember to check your voicemail periodically to make sure you aren't missing important calls and to clear out any spam calls that might fill your voicemail box to capacity.
- ✓ Stick a Pin on your mobile phone carrier's account



## What is SIM Jacking/Swapping?

### **SIM-Jackers Can Empty Your Bank Account with a Single Phone Call**

***Sim-Jacking is growing at such a rapid rate every year.***

- Technology has been a real godsend for fraudsters. Used to be you had to painstakingly recreate a valuable painting or convince hopeless marks to sign up to your pyramid scheme. The fraudsters usually had to be in-person to scam you.
- At its most basic level, a SIM Jacking/Swapping is when a scammer convinces your mobile phone carrier to switch your phone number over to a SIM card they own.
- SIM-jacking differs from other forms of hacking in that it does not require any technical know-how; all you need is a conman's skills of persuasion and a basic grasp of identity theft.
- The scammers are not doing it for prank call cover or to rack up long-distance charges.
- By diverting your incoming messages, scammers can easily complete the text-based two-factor authentication checks that protect your most sensitive accounts and that allows you to change your passwords.

### **How to Avoid It SIM Jacking/Swapping**

- **Stick a PIN On It**  
Every major US carrier offers you the option of putting a PIN or a passcode on your account. Take them up on it.  
Having one adds another layer of protection, another piece of information an attacker needs before they can compromise your identity.

### **Victim of a SIM Jacking/Swapping Attack**

Individuals who had their phone numbers stolen in a SIM swapping attack needs to follow the following procedure to minimize the potential damages:

- ✓ Contact your cellular service provider immediately to take back control of your phone number.
- ✓ After you regain access to your phone number, immediately change your account passwords.
- ✓ Immediately Check your checking and savings accounts and any other banking accounts, credit card, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution.

If the crooks have already taken control of one of your accounts or have already stolen some of your information, including but not limited to Social Security, credit card, or bank account numbers, you need to head over to [IdentityTheft.gov](http://IdentityTheft.gov) and follow the steps needed to protect yourself from identity theft.

**[FTC Issues Guidance on Protecting Against SIM Swap Attacks \(bleepingcomputer.com\)](http://bleepingcomputer.com)**



## Phone Scammers

**The more you know, the less likely you will become a victim.**

[Protect Yourself from Social Security Number Spoofing Scams | Federal Communications Commission \(fcc.gov\)](#)

**How to Recognize Phone scams and what to do**

[Phone Scams | FTC Consumer Information](#)

**Learn more about unwanted calls and what to do about them at [fcc.gov/calls](#), [Robocalls | FTC Consumer Information](#)**

**If you think you've been the victim of a spoofing scam, you can [file a complaint with the FCC](#).**

**Follow the helpful tips in the [Caller ID Spoofing | Federal Communications Commission \(fcc.gov\)](#)**

### **Social Security Scam:**

If you receive a suspicious call from someone alleging to be from the Social Security Administration (SSA) or Office of the Inspector General (OIG):

- You should report that information to the OIG online at [Report Fraud, Waste, or Abuse | Office of the Inspector General, SSA](#) or by calling (800) 269-0271, Monday through Friday, 10 a.m. to 4 p.m. Eastern Time.
- You can also report these scams to the Federal Trade Commission through a new site-specific to Social Security scams: [Identity Theft Recovery Steps | IdentityTheft.gov](#)
- Please report; The more we report, the more law enforcement can learn about the scammers and share this information with us, so we can be better prepared to not become a victim.

Read the [FCC Complaint Center FAQ](#) to learn more about the FCC's informal complaint process, including how to file a complaint and what happens after a complaint is filed.

### **Threatening Phone Scams Are Targeting Parents And Grandparents**

[Threatening phone scams are targeting parents and immigrants | FTC Consumer Information](#)  
[Grandparent scams in the age of Coronavirus | FTC Consumer Information](#)

### **Threatening Phone Scams Are Targeting Immigrants**

[Threatening phone scams are targeting parents and immigrants | FTC Consumer Information](#)

### **Federal Trade Commission (FTC)**

Learn about recent scams and how to recognize the warning signs. Read the FTC's most recent alerts or browse scams by topic.

<https://www.consumer.ftc.gov/features/scam-alerts>

## How to Block Unwanted call

### [How to Block Unwanted Calls | FTC Consumer Information](#)

<p><b>How to stop unwanted calls IF YOU USE VoIP</b></p> <p>Look into <b>Internet-based services</b>. Your carrier might be able to help.</p> <p>Not sure if your home phone uses the <b>Internet (VoIP)</b>? Check with your <b>carrier</b>.</p> <p>With blocking services, calls might be <b>stopped, ring silently, or go straight to voicemail</b>.</p> <p>Some services are <b>free</b>, but others charge a <b>monthly fee</b>.</p> <p>Report unwanted calls at <a href="http://ftc.gov/complaint">ftc.gov/complaint</a></p> <p>FEDERAL TRADE COMMISSION • <a href="http://ftc.gov/calls">ftc.gov/calls</a></p>	<p><b>How to stop unwanted calls ON A MOBILE PHONE</b></p> <p>See what <b>built-in features</b> your phone has.</p> <p>Download a <b>call-blocking app</b>.</p> <ul style="list-style-type: none"> <li>Some apps are <b>free</b>, but others charge a <b>monthly fee</b>.</li> <li>Some apps will <b>access your contacts</b>.</li> <li>Calls might be <b>stopped, ring silently, or go straight to voicemail</b>.</li> </ul> <p>See what services your <b>carrier</b> offers.</p> <p>Report unwanted calls at <a href="http://ftc.gov/complaint">ftc.gov/complaint</a></p> <p>FEDERAL TRADE COMMISSION • <a href="http://ftc.gov/calls">ftc.gov/calls</a></p>	<p><b>How to stop unwanted calls ON A LANDLINE</b></p> <p>See what services your <b>carrier</b> offers.</p> <p>Install a <b>call-blocking device</b>.</p> <ul style="list-style-type: none"> <li>Some use <b>blacklists</b> to             <ul style="list-style-type: none"> <li>stop unwanted calls</li> <li>divert calls to voicemail</li> </ul> </li> <li>Some use <b>whitelists</b> of approved numbers.</li> </ul> <p>Some services are <b>free</b>, but others charge a <b>monthly fee</b>.</p> <p>Report unwanted calls at <a href="http://ftc.gov/complaint">ftc.gov/complaint</a></p> <p>FEDERAL TRADE COMMISSION • <a href="http://ftc.gov/calls">ftc.gov/calls</a></p>
---	--	--

## [Avoid Spoofing Scams \(fcc.gov\)](#)

**FCC | CONSUMER CONNECTIONS**

### Avoid Spoofing Scams

Phone scammers often disguise their identity by using illegal spoofing techniques to send false information to your caller ID display. To trick you into answering, spoofers may use local area codes and numbers that look familiar. Or they may impersonate a company you do business with, such as a local utility, or even a government agency.

**Here are some good ways to avoid being spoofed:**

- Don't answer calls from unknown numbers.
- If you answer and it's not who you expected, don't hang on, hang up.
- If a caller asks you to hit a button to stop getting calls, just hang up.
- Never assume an unexpected call is legitimate. Hang up and call back using a number you can verify on a bill, a statement, or an official website.
- Be suspicious. Con artists can be very convincing: They may ask innocuous questions, or sound threatening, or sometimes seem too good to be true.
- Don't give out personal information – account numbers, Social Security numbers or passwords – or answer security questions.
- Use extreme caution if you are being pressured for immediate payment.
- Ask your phone company about call blocking tools for landlines or apps for mobile devices.
- Report spoofing scams to law enforcement, the FCC and the FTC.

**FC** Learn more at [fcc.gov/spoofing](http://fcc.gov/spoofing)



## A Few Other Items

### Wi-Fi

- **Never use a public Wi-Fi network.** Always use a Virtual Private Network (VPN). VPNs encrypt your internet connection, making it difficult for cybercriminals to intercept and steal your data. Never connect to public Wi-Fi without a VPN, and even then, avoid accessing highly sensitive information.  
<https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/securing-home-network//>
- Check with your internet or your mobile provider to see if they offer a free VPN service with your subscription.
- If you are looking for a free VPN, the TechRadar article "The best free VPN 202" is a great place to start to understand the pros and cons of free VPN services.  
<https://www.techradar.com/vpn/best-free-vpn>

### Establish a strong password for each online shopping account.

Be unpredictable and creative when creating a password. Always use fourteen or more characters consisting of upper-case letters, lower-case letters, numbers, and special characters to create a strong password.

Substitute traditional passwords with passphrases such as "welc0meH0MEFri\$end!"

You may want to consider getting a password manager—software that creates, stores, and syncs all of your logins across multiple devices.

Check with your internet or your mobile provider to see if they offer a password manager with your subscription.

If you are looking for a Password Manager TechRadar's article "Best password managers in 2021: Free and paid software to secure your passwords" is a great place to start.

<https://www.techradar.com/best/password-manager>

### Call Blocking Technology

Which type of call-blocking technology you use will depend on the phone: Check with your carrier to see what they have to offer.

- Cell phone
- Traditional landline
- A home phone that makes calls over the internet (VoIP)
- See what services your phone carrier offers and look online for expert reviews.
- For cell phones, you also can check out the reviews for different call-blocking apps in your online app store.



## For Parents and Caretakers

### NetSmartz Workshop

This is an excellent place for your children to learn how to become safer online.

<https://www.netsmartzkids.org/>

### NSTeens

Helping you make safer choices online. <https://www.nsteens.org/>

### National Center for Missing and Exploited Children

National Center for Missing and Exploited Children is the nation's clearinghouse and comprehensive reporting center for all issues related to the prevention of and recovery from child victimization; NCMEC leads the fight against abduction, abuse, and exploitation - because every child deserves a safe childhood.

<https://www.missingkids.org/home> <https://www.missingkids.org/education>

Tip Line: CyberTipline.com

1-800-The Lost

## Online Security

### *Federal Trade Commission (FTC) Online Security*

The internet offers access to a world of products and services, entertainment, and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves. Learn how to protect your computer, your information, and your online files.

[www.consumer.ftc.gov/topics/online-security](http://www.consumer.ftc.gov/topics/online-security)

Scammers use email or text messages to trick you into giving them your personal information. But there are several things you can do to protect yourself.

<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

Do Not Take the Bait

<https://www.consumer.ftc.gov/articles/phishing-dont-take-bait>

### National Cyber Security Alliance (NCSA) Online Safety Basics

*Learn how to protect yourself, your family, and your devices with these tips and resources.*

<https://staysafeonline.org/stay-safe-online/>

### *Securing Your Home Network*

<https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/securinghome-network/>



## Protecting Your Identity

### **Federal Trade Commission (FTC) Protecting Your Identity**

While identity theft can happen to anyone, there are some things you can do to reduce your risk.

<https://www.consumer.ftc.gov/topics/identity-theft>

## Ransomware

Here are some tips individuals can take to avoid a ransomware attack. Please visit the FBI, CSA, and FTC sites below to obtain additional information on how to avoid ransomware and what to do if you are a victim of a ransomware attack.

*Do not click on emails you do not know who they are from*

*Make sure your PC/Laptop operating system, is patched*

*Patch your software*

*Keep your PC/Laptop clean*

*Think before your click*

*Ensure anti-virus and anti-malware solutions are set to automatically update and conduct regular scans.*

*Back up data regularly and verify the integrity of those backups. Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware, you will be able to restore the data from a backup.*

→ *Use Peter Krogh 3-2-1 rule as a guide to backing up your data*

- ✦ *The rule is: Keep at least three (3) copies of your data and store two (2) backup copies on different storage media, with one (1) of them located offsite.*
- ✦ *Secure your backups. Make sure they are not connected to the computers and networks they are backing up. - Veeam Software*

**FBI** <https://www.fbi.gov/investigate/cyber>

Ransomware Overview: <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware>

### **Cybersecurity and Infrastructure Security Agency CISA**

Ransomware Overview: <https://www.us-cert.gov/Ransomware>

### **Federal Trade Commission (FTC)**

Ransomware Brochure & Quiz: <https://www.ftc.gov/tips-advice/business-center/smallbusinesses/cybersecurity/ransomware>



### ***What to Do If You Experience Ransomware***

#### **FBI**

1. Report the incident to FBI's Internet Crimes Complaint Center <https://www.ic3.gov/default.aspx>
  - ✦ Include any contact information (like the criminals' email address) or payment information (like a Bitcoin wallet number).
2. You can report it to your local FBI Field Office: <https://www.fbi.gov/contact-us/fieldoffices/field-offices>

#### **Cybersecurity and Infrastructure Security Agency (CISA)**

1. Victims of ransomware should report it immediately to CISA at <https://www.uscert.gov/forms/report> or a local FBI Field Office, or Secret Service Field Office.

#### **Secret Service Field Office:**

1. Secret Service Field Office: <https://www.secretservice.gov/contact/field-offices/>

### **How to Report Phishing Scams**

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

**Step 1.** If you got a phishing email, forward it to the Anti-Phishing Working Group at [reportphishing@apwg.org](mailto:reportphishing@apwg.org).

If you got a phishing text message, forward it to SPAM (7726).

**Step 2.** Report the phishing attack to the FTC at [ftc.gov/complaint](http://ftc.gov/complaint).



## How to Report Cybercrime

### Federal Trade Commission (FTC)

- ✦ [IdentityTheft.gov](https://www.ftc.gov/identity-theft) to report and recover from identity theft and get a recovery plan, and put it into **action**.

### FBI: Internet Crime Complaint Center

- ✦ FBI Field Office: <https://www.fbi.gov/contact-us/field-offices/field-offices> ✦  
<https://www.ic3.gov/default.aspx>

### Cybersecurity and Infrastructure Security Agency (CISA)

1. Victims of ransomware should report it immediately to CISA at <https://www.uscert.gov/forms/report> a local FBI Field Office or Secret Service Field Office.

### Other Local Law Enforcement Office

1. Secret Service Field Office: <https://www.secretservice.gov/contact/field-offices/>

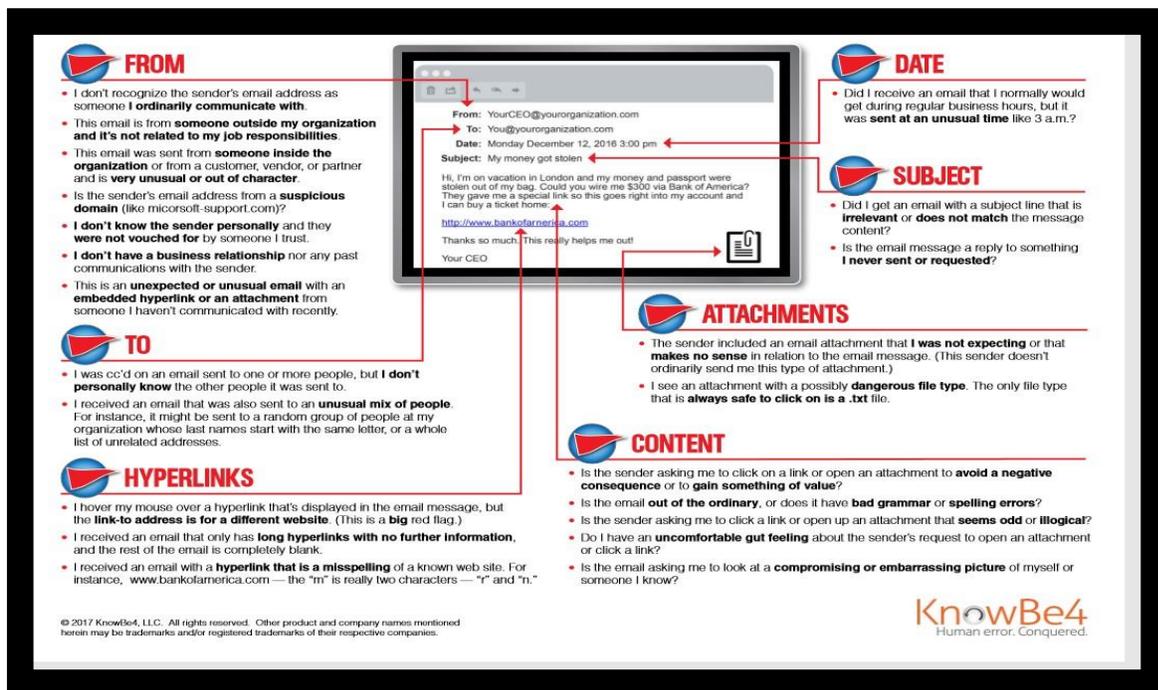
## Be Smart Be Vigilant on How You Create Your Password By

1. Remember, the longer the password; the better, so start with using 12 Characters Password length
2. Being unpredictable and creative
  - Includes Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.
3. A strong passphrase is a random combination of words that are meaningless together.
4. Avoid Bunching Numbers and Symbols Together
  - One good password practice that often goes overlooked is to spread numbers and symbols throughout the password instead of bunching them together, which makes it easier for the password to be hacked.
5. Refrain from Using Dictionary Words
  - Stay away from obvious dictionary words and combinations of dictionary words. Sophisticated hackers have programs that search through tens of thousands of dictionary words.
  - Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house12!" is a terrible password. "Redhou1!" is also very bad.
  - Having an 'obvious' password like "Pas\$w0r1" makes it easy for hackers to hack: this password is not strong in today's world because hackers have sophisticated ways of cracking a password.
  - What makes "Pas\$w0r1" a weak password; it is a dictionary word where the first letter is capitalized, the "s" is replaced with \$, the number is at the end. B00k123! is another

password easy to hack: What makes "B00k123!" a weak password; is it a dictionary word where the first letter is capitalized, the letters "oo" are replaced with zeros "00", the numbers are sequential "123".

- A three-letter sequence that just happened to spell a dictionary word - such as "cat," but the password is Dcatt4674!& works well
6. Please create unique passwords that steer clear of personal information like company names, usernames, social security numbers, nicknames, date of birth, and a relative's name.
  7. Use Different Passwords for Different Accounts
    - It can be tempting to use the same password for every account, so we do not forget our passwords. However, this makes it easier for hackers to break into a multitude of accounts. Diversify your passwords by using a different password for every account.
  8. Change your password if you think it has been compromised.

## Do Not Click on Anything Without First Checking For



**FROM**

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like [microsoft-support.com](mailto:microsoft-support.com))?
- I **don't know the sender personally** and they were **not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

**TO**

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

**HYPERLINKS**

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "r" and "n."

**DATE**

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

**SUBJECT**

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

**ATTACHMENTS**

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

**CONTENT**

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4  
Human error. Conquered.

## Secure Your Mobile Phone

With the growing use of mobile phones to conduct business, shop, and more, mobile devices are becoming a major cause of concern in the security community. Help protect your phone and other mobile devices from hackers by securing your phone with a strong password. Or, better still, use fingerprint or facial recognition passwords to help outwit the hackers.

# 20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

**WiFi**

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

**Apps**

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

**Browser**

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.



**Bluetooth**

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

**Smishing (phishing via SMS)**

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

**Vishing (voice phishing)**

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.

© 2018 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

