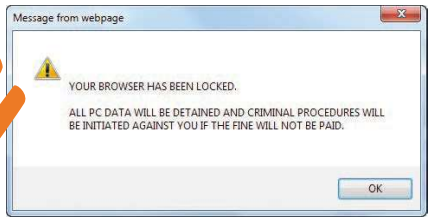
CYBERSAFETY and You



Cybersecurity attacks are flourishing—from our own community all the way to the federal government. Learn to recognize scams and protect yourself against nefarious criminals to help ensure you don't fall victim.

BY DEBORAH DOTSON

During the past year, the use of digital devices and social media has increased exponentially as we long for a connection with our fellow humans. With the rise in use of these tools comes increased cybersecurity crime and risk. Regrettably, our senior age group is targeted more frequently as criminals prey upon our humanity and kindness. Simply put, because we are good people, we make it too easy for them to be bad people! Follow these safety measures to reduce your risk of becoming their next victim.

Social Engineering by Cybercriminals

"Social engineering by cybercriminals" is a phrase applied to a wide range of malicious activities perpetrated through human interactions. These methods use psychological manipulation to trick users into making security mistakes or giving away sensitive information. This type of crime focuses on human emotions and human nature. It often can occur in more than one step, where the person first gains some background information or finds a weakness and then acts.

- **Fear:** Inspired via a phone call, during which the caller tells you a relative needs help in another state or country, you've committed a crime, you owe the IRS or there's a problem with your

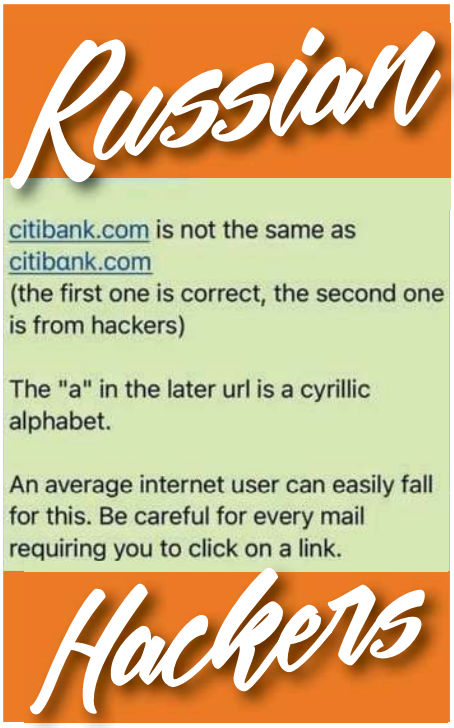
Unless you are certain the email came from a reputable source, don't click or open it. It may contain a virus that will infect your computer or device (also see malware).

bank account. All of these scenarios would immediately cause you to become fearful of wrongdoing, and cybercriminals prey on that stress and anxiety to get you to surrender to their requests. This activity is called "vishing" and can be coupled with pretexting.

- **Greed:** Who wouldn't want to invest $10 and get back $10,000? Cybercriminals manipulate basic human emotions of trust and greed to convince you that you can get something for nothing. A sensibly worded email asks victims to provide their bank account information; after doing so, funds will be transferred the same day. This also can include in-person crime, where a person with a lottery ticket tells a story to get you to cash it for them or asks you to buy gift cards on their behalf and you'll be financially rewarded for your help. This type of activity is called "baiting," "phishing," "quid pro quo" and "pretexting."
- **Curiosity:** Humans are naturally curious about news and current events. Emails with attachments claiming to hold the "real story" about a plane crash, a shooting or a robbery entice you to open it to read the content—and then a virus is downloaded and embedded, and immediately infects your computer.
- **Helpfulness:** Humans want to trust and help one another, so these emails implore you to help someone you know or, if you are working, someone at your company.
- **Urgency:** During the past year, you've probably ordered something (or many things) online. If you received an email from this company telling you that if your credit card information isn't confirmed immediately your data is at risk of being stolen by criminals, you'd want to ensure that didn't happen by responding without thinking.

Baiting and Phishing

Facebook is a big place for cybercrime. Please do not play those "name" games that ask you to click and answer questions. Clicking on the link alone puts you and all your Facebook friends and family at risk. These "games" seem fun and harmless, but they are not. They are called "click-bait" because they are baiting you just like a worm on a fishing line baits fish! Warn your friends about the dangers of playing these games, too. It's very easy



for this information to get into the wrong hands—cybercriminals are very sophisticated.

Another form of baiting and phishing is receiving an email asking you to click a link for more information or open an attachment. One example is an email received from a service that alerts you to something requiring immediate action, such as a password change. Unless you are certain the email came from a reputable source, don't click or open it. It may contain a virus that will infect your computer or device (also see malware).

To check who really sent you the email, hover your cursor (the little arrow) over the sender's name, and right click to see who actually sent it.

Phishing is done in many ways, including via deceptive emails that ask you to provide more information, text messages sent to your phone or requests to visit websites, all designed to

steal your personal information. Taking precautions is of the utmost importance, but it's not realistic in most cases to just stop using email, social media or your computer to find information. Taking time to do a little investigation can save you hours of angst in trying to undo the trouble caused. Make sure the email sender is legitimate by right clicking the address, and read the content, as it often contains spelling errors or it is grammatically incorrect. You can even call the sender to see if they sent the email to you. Don't open attachments unless you are 100% sure you know where they came from and trust the senders.

Vishing/Pretexting

This type of cybercrime comes into play when someone calls pretending to be someone else (law enforcement, bank/tax officials or coworkers). Cybercriminals know these calls will frighten seniors and spur them to act quickly to avoid arrest or other risk. One common example of this scam is a "call" from the IRS about owing money or claiming a lien against you is filed. The IRS never calls citizens! This federal agency always uses certified mail to communicate with intended recipients. Another example features a caller who claims to be a grandchild who is stuck somewhere and needs money asap. The best way to protect yourself here is to block the number on your phone, erase the voicemail and add a free app from your service provider to indicate spam-risk phone numbers.

Malware

Malware, sometimes called "hacking," is a common, long-term problem that continues to grow due to the sophistication of the criminals and the tech they use.

In a workplace environment, malware can be added to an email attachment, which is opened by the employee, and sends the "poison" throughout the whole network system. Malware can halt business completely until it is resolved. Typically, cybercriminals hold the system for ransom, telling a company they will extract the malware for a fee. This is called ransomware. Even our federal government was recently "hacked" in this way.

Individuals may click a link that installs the malware or open an email attachment that has an embedded virus that can shut down your entire computer and erase your files. This will require you to take your computer to a company that specializes in these repairs. So, although the malware installer may not make money,

FIGHT CYBERCRIME!

The only way to avoid cybercrime is to never use the internet or a smartphone, which is not realistic for most. While nothing is 100% secure, using the internet and digital devices safely is possible by following a few rules and using good judgment.

- Take the time to regularly update your computers, firewalls and antivirus software and set them to perform frequent scans.
- Read before you click.
- Set alerts and check your account frequently if you bank online.
- Log on to your bank from your home network—never do it on a public computer.
- Change passwords monthly for all of your accounts accessed online, and don't use easy-to-guess information.
- Consider using two-factor authentication, which uses your password and a special code sent to you to log in to an account.
- Ask someone you trust to review emails if you are unsure about something you read or see, or receive from a third party.

you lose money via the repair company's charges.

The best way to avoid malware is to never click on any links or attachments. Installing a good firewall and antivirus software on your devices also are musts. A firewall is the first defense against potential cyberattacks. Antivirus software also is important, but relying on a single tool is not enough now. Set up these tools to update and scan your device frequently. Regularly back up your data to a cloud-based service or an external storage device.

Scareware

Scareware usually appears on a desktop computer in the form of legitimate-looking popup banners showing messages like "Your computer may be infected with harmful spyware programs." If you click the message to determine the issue, you may be directed to install something to "fix" the problem, which is actually malware. It also can direct you to another site for more information, which then infects your computer or sends your information to a third party.

Antivirus software and firewalls don't always stop this, either, so never fall for this trick. The only popup you might see from antivirus/firewall software is a message telling you that a device scan is about to begin. Other than that, never click or install anything from a popup message.

Spyware

Spyware describes software installed on your device without your knowledge or permission. This malicious behavior intends to collect personal data and send it to another entity in a way that harms the user in any number of ways, via a stolen bank account number, a birthdate or even a social security number. Typically, good antivirus software will protect against spyware, but other add-on protections are designed specifically for spyware.

Quid Pro Quo

This "favor for a favor" situation is where the cybercriminal will ask you to do something in return for something else. One example is the "Prince in Nigeria" email, which asks to send you money, but you have to give them access to your bank account. Most people are aware of this scam, as it has been around for years, but these letters are getting more sophisticated, and now they may say they are from your bank or a credit card company.

Honeytrap

The honeytrap scenario, where a woman was used to trick a man into giving up information by feigning interest comes from old-fashioned spy tactics. In the cyberworld this is common on dating websites where a person uses a fictitious profile to interact with a potential victim. All ages are potential victims but the scam is most prevalent in the senior community due to pandemic-caused loneliness. The best advice here is to be very careful and not give any money or personal information to someone you haven't met or investigated.

Deborah Dotson, M.Ed., is currently an adjunct professor at two major universities where she teaches a variety of undergraduate technology courses. As a lifelong learner, with three decades in executive-level business management experience in healthcare and instructional technology, she turned her focus to K-12 education, where she trained and coached teachers on the effective use of technology in their classrooms and served as a common-sense media certified educator, working with students on digital citizenship and internet safety. Deborah is also a director on the Third Laguna Hills Mutual board and a member of Computer Using Educators, and actively consults on instructional design and using technology in education.