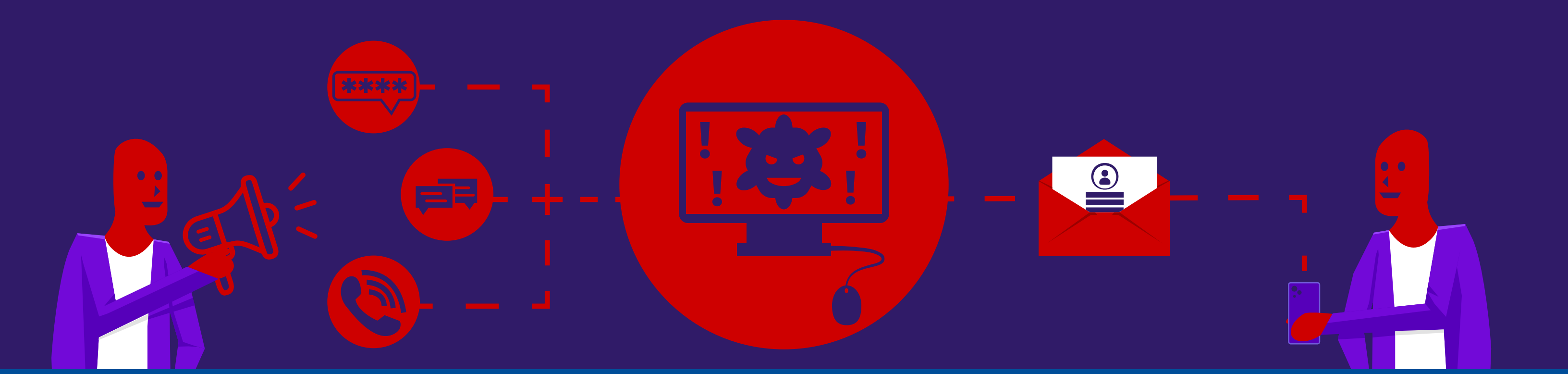

PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, ecommerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts

HOW CRIMINALS WILL LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- *"We suspect an unauthorized transaction on your account. To ensure that your W account is not compromised, please click the link below, and confirm your identity."*
- *"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."*
- *"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."*

SIMPLE TIPS:

- **Play hard to get with strangers.** Links in email and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email.
- **Think before you act.** Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy.
- **Protect your personal information.** If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you.

OKLAHOMA Education

Data Privacy Week

Privacy@sde.ok.gov

ONLINE SAFETY TIPS

We're constantly connected – whether it's text messaging, apps, social media, online games, website or emails – and that makes us all vulnerable to thieves looking to take advantage of us when we least expect it.

Thieves will go to any length to learn about you. Asking yourself these questions will help keep your personal information safe:

QUESTIONS TO ASK YOURSELF

- **Am I posting sensitive information?** This means addresses, phone numbers, your birthdate, Social Security number, driver's license number or financial information.
- **Should I share this?** Be careful posting details about your life, and don't answer questions – online or over the phone – from anyone you don't know asking personal questions.
- **What are the privacy settings on my accounts?** Look through the settings of the social media you use to be sure only people you absolutely trust see your posts.
- **Should I click** Unexpected links and attachments in messages might contain viruses or spyware that the sender doesn't even know about. Check with the sender first. If you don't know the sender, just trash the message.
- **Is this site legitimate?** Malicious websites can look identical to trusted sites, but the URL or email address might use a different spelling or domain (e.g., .net instead of .com). When in doubt, avoid the website until you're 100% sure.
- **Is my software up to date?** Check to be sure you're running the latest operating system, anti-virus software and web browsers.
- **Is it too good to be true?** Free games and other things might be tempting, but they can come at a cost to your privacy. Only download from trusted sources, even if you might have to pay.
- **Are my passwords safe?** Be sure your passwords include a mix of upper and lowercase letters, numbers and symbols. Make them hard enough that someone can't guess them, and don't share them with anyone.
- **Am I using free Wi-Fi?** Many public Wi-Fi hotspots – like at libraries, coffee shops and malls – aren't secure and might not protect your passwords, messages, photos and other date. Check with an employee before connecting.

OKLAHOMA Education

Data Privacy Week

Privacy@sde.ok.gov

IDENTITY THEFT AND INTERNET SCAMS

Today's technology allows us to connect around the world, to bank and shop online, and to control our televisions, homes, and cars from our smartphones. With this added convenience comes an increased risk of identity theft and Internet scams.

#BeCyberSmart on the Internet—at home, at school, at work, on mobile devices, and on the go.

PROTECT YOURSELF FROM ONLINE FRAUD

Whenever you're online, you're vulnerable. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

- Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar— this signifies a secure connection.
- When you find yourself out in the great "wild Wi-Fi West," avoid free Internet access with no encryption.
- If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.
- Don't reveal personally identifiable information such as your bank account number, SSN, or date of birth to unknown sources.
- Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

PROTECT YOURSELF FROM ONLINE FRAUD

- Double your login protection. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in.
- Shake Up Your Password Protocol. According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites.

OKLAHOMA Education

Data Privacy Week

Privacy@sde.ok.gov

PERSONAL INFORMATION IS LIKE MONEY

Information about your kids, such as the games they like to play and what they search for online, has value – just like money. Talk to your kids about the value of their information and how to be selective with the information they provide to apps and websites. Have a discussion about what types of information they should share, and what types of information (such as addresses, photos, phone numbers, etc.) they should not share.based on information they found online.

WHAT HAPPENS ONLINE STAYS ONLINE

Help your children understand that any information they share online can easily be copied and is almost impossible to take back. Teach them to consider who might see a post and how it might be perceived in the future.

FIND OUT MORE ABOUT DATA, PRIVACY, AND TOOLS TO KEEP YOUR INFORMATION SAFE.

SCAN HERE

Privacy@sde.ok.gov

OWN YOUR ONLINE PRESENCE

Start the conversation about the public nature of the Internet early. Learn about and teach your kids how to use privacy and security settings on their favorite online games, apps and platforms. Take a moment to configure them together– explaining why you are restricting some features (such as location tracking). Post only about others as you would like them to post about you Remind children and family members about the golden rule and that it applies online as well. What they do online can positively or negatively impact other people.

OKLAHOMA Education

Data Privacy Week

KEEP PERSONAL INFO PERSONAL

Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data or commit other crimes such as stalking.

ONCE POSTED, ALWAYS POSTED

Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70 percent of job recruiters rejected candidates based on information they found online.

BE AWARE OF WHAT'S BEING SHARED

Be aware that when you post a picture or video online, you may also be sharing information about others or personal details about yourself like where you live, go to school or hang out.

KNOW AND MANAGE YOUR FRIENDS

Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That doesn't mean all friends are created equal. If you're trying to create a public persona as a blogger or expert, create an open profile or a "fan" page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) up to date with your daily life. Also, you don't have to accept friend requests from everyone. If you don't know someone, it's perfectly fine not to accept their request to connect.

FIND OUT MORE ABOUT DATA, PRIVACY, AND TOOLS TO KEEP YOUR INFORMATION SAFE.

SCAN HERE

Privacy@sde.ok.gov

OKLAHOMA Education

Data Privacy Week