Adult Education

April is National Financial Literacy Month, which is designed to create awareness about the importance of personal financial education. Throughout the month, we will be exploring different financial education topics with specific age-minded activities and links, designed for your use at home.

It seems that everything we do today relies on computers and the internet. We communicate, we are entertained, we rely on transportation navigation, we shop, we search for general information, and the list goes on and on. How much of your daily life relies on technology? Do you reach for your smartphone or tablet right away each morning or are you more of a casual user of technology? It is likely that much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system (like your credit card companies for instance).

Because so many people rely on the internet, it is important to be aware of the risks and scams that threaten our online security. How to spot and avoid scams goes along with staying secure online. Providing these "bad actors" with our personal information can lead to unfortunate consequences.

Wings
FINANCIAL
FOUNDATION

Cybersecurity

Cybersecurity-is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

To minimize the risks of cyberattacks, follow these cybersecurity best practices:

1. Keep software up to date
2. Run up to date antivirus software
3. Use strong passwords (16 characters or more, consider using a pass phrase)
4. Change default usernames and passwords
5. Implement multi-factor authentication (MFA)
6. Implement VPNs for all network connections. (Virtual private network)
7. Install a firewall
8. Be suspicious of unexpected emails
9. Look for lock sign on website when browsing the internet

- What are the risks to having poor cybersecurity? In business, the loss of customer and stakeholder trust can be the most harmful impact of cybercrime. The public does not want to do business with a company that has had a data breach. Poor cybersecurity can also cause electrical blackouts, military and national security failures and can result in the theft of valuable, sensitive data like medical and financial records.

Malicious code (Malware) is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Vulnerabilities are flaws in software, firmware or hardware that can be exploited by an attacker to perform unauthorized actions in a system. Find more information about malware, including how it gets on your devices, with this article: https://consumer.ftc.gov/articles/how-recognize-remove-avoid-malware

Wings FINANCIAL FOUNDATION

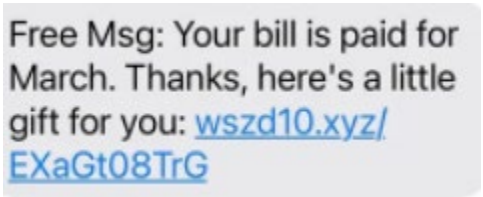
Recent Scams & Examples

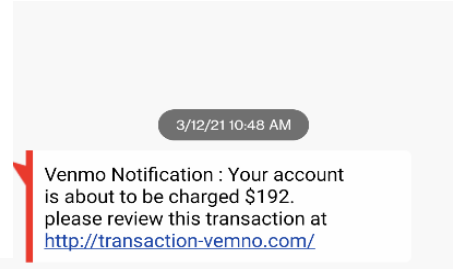
In person, it's fairly easy to recognize when someone is up to no good. However, as the world continues to digitize, new dangers may lurk in our email inboxes, our favorite websites and our social media accounts. Cybercrime can do irrevocable harm to our financial well-being and peace of mind. If you have never fallen victim to a scam, you may think it will never happen to you, until it does. Being able to understand and identify the scams that are being run is extremely helpful in avoiding becoming a target and falling prey to these "bad actors".

Resources:

1. Internet Crime Complaint Center- www.ic3.gov/
   Latest news releases by the FBI, filing a complaint with the Internet Crime Complaint Center, FBI cyber strategy, ransomware, consumer alerts, industry alerts, elder fraud, and scams
2. Readers Digest 10 Online Scams to Know and Avoid - https://www.rd.com/list/how-to-avoid-online-scams/
3. Protecting Your Kids Online- Protecting Your Kids — FBI (www.fbi.gov/scams-and-safety/protecting-your-kids)

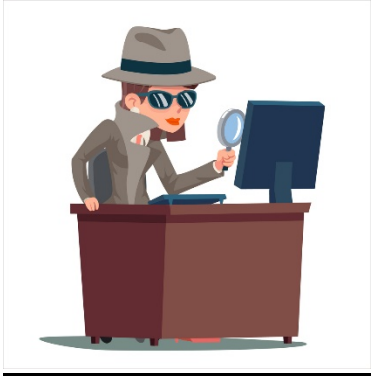
Text messages are the newest form of phishing, called Smishing. The uptick in spam messages that mobile phone users are receiving comes after the US government doubled down on its fight against robocalls. Here are a couple of examples, notice they both contain a link to lure you:





Wings FINANCIAL FOUNDATION

Recent Scams & Examples



Top Scams

1. Free Trial Offers-A free offer is made with hidden obligations to continue service
2. Your computer is infected!-A window pops up on your screen, hijacking your computer
3. A nearby imposter-Using available free Wi-Fi while a nearby imposter is mining your computer
4. Text messages received where scammers hope you will click to investigate further
5. Charity scams-Do your homework before giving to a new-to-you charity
6. Romance scams-Your new love online is a scam artist and would love to take your money!
7. Scam-azon-You believe that using a trusted sight will give you a quality product, not always
8. Travel scams-Great offers for cheap travel that have many hidden costs in the fine print
9. Online retailer scams-Products offered at deeply discounted prices through a social media app
10. Government imposters that threaten your arrest or an unpaid tax bill or SSN identity theft
11. Unsolicited emails from reputable companies asking for account information verification
12. Disaster relief scams will use a tragedy or natural disaster, to con you into a donation
13. Fake shopping websites try to mimic another familiar company offering great deals
14. Tech support scams can target people by computer hijacking or by phone
15. Fake antivirus software ads and pop-ups try to make you believe your computer is infected
16. Pre-approval notice for a credit card or bank loan promising instant approval
17. Debt relief and credit repair scams claim to relieve your debt or repair your credit score

For more scam information, see the articles and links provided on the previous page. You can also subscribe to government websites and the FTC.gov website for email notifications of new information.

Wings FINANCIAL FOUNDATION

Ransomware

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.
Ransomware Fact Sheet: www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware. Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers.

Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Tips for Avoiding Ransomware

The best way to avoid being exposed to ransomware—or any type of malware—is to be a cautious and conscientious computer user. Malware distributors have gotten increasingly savvy, and you need to be careful about what you download and click on.
Other tips:

- Keep operating systems, software, and applications current and up to date.
- Make sure anti-virus and anti-malware solutions are set to automatically update and run regular scans.
- Back up data regularly and double-check that those backups were completed.
- Secure your backups. Make sure they are not connected to the computers and networks they are backing up.

Wings FINANCIAL FOUNDATION

April 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people

Getting Personal With Security

- **Top Tips for Personal Security**
- **5 Security Tools Everyone Should Use**
- **Common Scams to Watch Out For**

Top Tips for Personal Security

Let's shift our focus from how you can help our organization remain secure to how we can help you stay secure. Here are a few tips to avoid data theft, financial loss, or malware infections:

Stay alert for phishing attacks

Phishing is one of the most common attacks you'll encounter both at work and at home. Stay on the lookout for common warning signs like bad grammar, misspellings, threatening language, and a sense of urgency. Don't click on any links or download attachments that came to you randomly.

Think like a scammer

Before sending someone money or revealing personal information, think through the situation from a scammer's perspective. Does it seem like a good way to defraud someone? Does anything seem out of the ordinary? Trust your instincts and avoid assuming someone is who they claim to be.

Stay safe on social media

Unless you're trying to build a personal brand, it's best to set your social media accounts to private and always vet anyone who wants to connect with you. Cyber criminals search public profiles for any information that might be useful to carry out scams.

Protect your mobile devices

From messaging to banking to social media, our smartphones open a lot of digital doors. If available, enable remote services that allow you to locate a missing device or erase all data when the phone can't be recovered. Only download applications from trusted sources, and keep an eye on the permissions any software asks for.

Replace your passwords with passphrases

We need our passwords to be easy to remember, yet hard to crack. Passphrases accomplish this by forming a sentence (at least 16 characters long) that is meaningful to you and only you. Obscure song lyrics or book quotes, for example, make for great passphrases.

5 Security Tools Everyone Should Use

Password Managers

The problem: most of us have dozens upon dozens of passwords to remember.

The solution: a program that remembers them for you and stores them behind one master password.

That's the job of a password manager—software that can create, store, and sync your login credentials across multiple devices. Be sure to make your master password strong, unique, and memorable.

Multi-factor Authentication (MFA)

The problem: if your password gets stolen, you could lose control of your account.

The solution: requiring a second code before access to an account is granted.

Even if you enter the correct username and password for an account, MFA prompts for a second code that's sent via some other communication method. Enable it wherever possible.

Remember, here at work, always follow policies and never install any software or applications unless they've been explicitly approved.

Ad Blockers

The problem: online advertisements are annoying and can be dangerous.

The solution: browser plugins that block most advertisements and popups.

Cyber criminals can inject legitimate websites with malicious ads. Ad blocking plugins automatically eliminate most of them and will make your browsing experience more enjoyable and more secure.

Antivirus Software

The problem: computer infections lead to data theft and/or poorly performing devices.

The solution: software that detects and removes malicious programs or code.

While free versions of antivirus programs work well, paid options have many extra features you might find valuable. Do some research, find one that fits your needs, and install it on all devices.

Alternative Browsers

The problem: many websites and web browsers track and store information about users.

The solution: using an alternative browser that focuses on privacy instead of data collection.

If you want to avoid the potential privacy concerns related to your internet activities, consider using a browser that, by design, blocks internet trackers and doesn't store browsing habits.

Common Scams to Watch Out For

Cyber criminals are opportunistic. They'll gladly target individuals just like they do large organizations. Let's explore a few common scams that anyone might encounter.

The fake rental property

Imagine paying a deposit on a new rental home, only to find out later that someone already lives there. Rental scams usually involve a fraudulent listing of a real property. The scammers sometimes figure out how to copy keys (or break into the home to unlock it) so the victim gets an opportunity to view the home in person.

The caller who demands payment by gift cards

The caller might claim to be from a power utility company or a financial collection agency and threaten you with fees or account closures. Instead of a traditional payment, they ask you to purchase gift cards and provide the relevant information on the cards.

The extortionist

Fear is the most powerful ingredient in extortion scams. They typically involve an email with a threatening subject line like "I saw what you did." The messenger claims they used remote desktop software to record your screen and your webcam. They then threaten to send the video to all of your contacts unless you immediately pay the scammer.

The one where your account has been suspended

This common phishing scam comes via an email that features logos and contact information from a real business. The message states that your account has been suspended due to fraudulent activity and that you must update your login credentials, or the account will be closed permanently.

In all cases, you can easily avoid becoming a victim by:

- *Using situational awareness and common sense*
- *Verifying someone's legitimacy before sending payment*
- *Slowing down if a situation is emotionally triggering or unrealistic*
- *Thinking before clicking or downloading anything*

Steps to take if you experience identity theft

Free Help at IdentityTheft.gov

Get a personal recovery plan that walks you through each step.
Create an **identity theft affidavit** that you can review and update at any time.
Get **customized pre-filled letters** to send to credit bureaus, businesses, and debt collectors.
Return anytime to **update your plan** and **track your progress.**
Get advice about what to do if you're affected by **specific data breaches.**

Visiting IdentityTheft.gov is your one stop shop for the process of recovering and rebuilding after falling victim to fraud. Take immediate action if you become aware you are a victim.

What to do right away:

- Call the companies where you know fraud occurred
- Place a fraud alert with the credit bureaus and get a copy of your credit report
- Report ID theft to the Federal Trade Commission (FTC)
- File a report with your local police department

What to do next:

- If new accounts were opened in your name, close them
- Remove bogus charges from your accounts
- Correct your credit report if necessary (Equifax, Experian, TransUnion)
- Consider adding an extended fraud alert or credit freeze

Other possible steps:

- Report a misused Social Security Number
- Stop debt collectors from trying to collect debts you don't owe
- Replace government-issued IDs if necessary

Wings FINANCIAL FOUNDATION