High School 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).

As a high school student, you have relied on the internet more than ever due to the shift to remote learning in 2020. The last two years have certainly been more challenging to some than others. But it has taught us that being safe online and protecting our personal devices, is more important than ever.

Wings FINANCIAL FOUNDATION

Privacy Tips for Teens

1. What you post online can last a lifetime.
2. Be aware of what's being shared, personal details like location.
3. Use strong and unique passwords of at least 16 characters, password managers are helpful.
4. Post only about others as you would like to have them post about you.
5. Learn about privacy and security settings on your favorite online games and apps.
6. Know what's being collected, who is collecting it and how it will be used.
7. Secure your devices with strong passwords or touch ID features.
8. Public WiFi hotspots are not secure, anyone can see what you're doing.
9. Turn off WiFi and Bluetooth when not in use, so location trackers cannot work.
10. Delete anything you receive that looks weird or is unexpected.
11. Use encrypted websites**: Use** only websites with 'http**s**' in their URL and a padlock icon next to it. The '**s'** stands for 'secure' (encrypted), which means that any data leaked or obtained by unauthorized parties is unusable.
12. Check the privacy policy of apps**: iOS** apps enforce all users to communicate through https, but the same cannot be guaranteed for Android apps. It's best to either check the privacy policy of each tool or inspect the website for an official stamp from a data protection organization.
13. Use a VPN, especially when connecting to shared networks**.** It protects and encrypts your internet traffic.
14. Be vigilant with phishing and Smishing attempts. Do not click on attachments or links, even if it looks like a reliable source. Go to your account to manage any issues.
15. Keep app's and device operating systems updated. This includes anti-virus software.

Wings FINANCIAL FOUNDATION

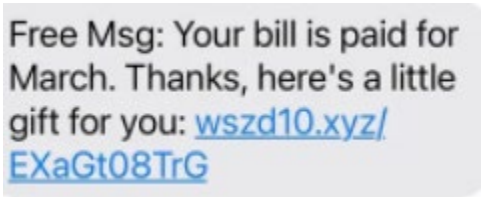
Recent Scams & Examples

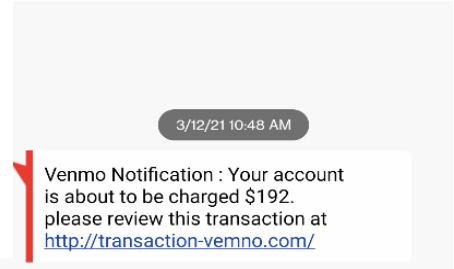
In person, it's fairly easy to recognize when someone is up to no good. However, as the world continues to digitize, new dangers may lurk in our email inboxes, our favorite websites and our social media accounts. Cybercrime can do irrevocable harm to our financial well-being and peace of mind. If you 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)

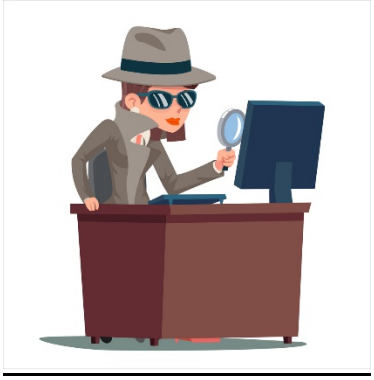
Text messages are the newest form of phishing, called Smishing. The uptick in spam messages that mobile phone users are receiving comes after the US government doubled down on its fight against robocalls. Here are a couple of examples, notice they both contain a link to lure you:





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

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

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

Test Your Password Knowledge

- A password should be between 8-16 characters. It should contain a combination of uppercase, lowercase, numbers, and special characters.
- Do not use words that are easy to guess, such as your name or your pet's name.
- Avoid common words and number combinations. Examples would be Password or 12345.
- Do not use the same password twice! Create a new password for every account, game, app etc.
- Change your passwords at least every six months.
- Do not share your passwords!

Carefully review each password below and circle whether the password is a strong or weak password.

1. L@!!k3L!f3W4	Strong	Weak
2. Sam@2013	Strong	Weak
3. spike1234	Strong	Weak
4. $pR!te#14*&*!	Strong	Weak
5. April152010@	Strong	Weak
6. Luv2w!m@1#	Strong	Weak
7. Football#1fan	Strong	Weak

Strong passwords: 1, 4 & 6

Wings FINANCIAL FOUNDATION

Cybersecurity Word Scramble

1. IFIW _____
2. SCMAS _____
3. CEIEDV _____
4. FUADR _____
5. TAESFY _____
6. SPEYARW _____
7. TENTERIN _____
8. SPRASWDO _____
9. BRYEC AWASEESNR _____
10. REMLAAW _____
11. NLNIOE _____
12. RCEAHK _____

Wings FINANCIAL FOUNDATION

Cybersecurity Word Scramble KEY

1. IWIF __Wifi_____
2. SCMAS __Scams_____
3. DCVEEI __Device_____
4. RADUF __Fraud_____
5. YFESTA __Safety_____
6. EASWRYP __Spyware_____
7. NEITTREN __Internet_____
8. SODRWPAS __Password_____
9. BECYR SRAWENSAE __Cyber Awareness_____
10. REMLAAW __Malware_____
11. NNLIOE __Online_____
12. CEAKRH __Hacker_____

Wings FINANCIAL FOUNDATION