FINANCIAL LITERACY MONTH

Middle School Education

It is week three of National Financial Literacy Month! This week's topic is Cybersecurity. According to wehavekids.com, 70% of students in grades 6-8 are regularly on the web. More and more of what we do daily relies on technology devices and the internet. Although the internet can be a great resource for kids, there are a lot of potential dangers and risks.

If you're a parent or guardian, you can help keep your kids safe by talking to them about their internet use**,** teaching them about online dangers, and learning everything you can about the internet so you can make informed decisions.

Tips for Parents

- Discuss internet safety and the importance of being aware and alert.
- Keep the computer or iPads in an open area. This will allow parents and guardians to see what apps, games, etc. children are accessing. In addition, kids will be more likely to make good choices and create safe habits when they are in an open area with adults present.
- Use parental controls. Parental controls are available on almost every device. These controls will allow you to restrict access to certain games and apps.
- Set time limits for all devices. Limiting your child's screen time will help eliminate online risks.

Here is a helpful article that you and your children can review together.

https://kidshealth.org/en/parents/net-safety.html

Wings FINANCIAL FOUNDATION

Password Safety

What is a password?

It’s a secret word or phrase that helps you get onto an app, game, website, or device!

Having a strong password is the first step to protect yourself. The stronger your password, the more protected your computer will be from hackers and malicious software. Here are some simple tips on how to create a strong password:

- 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! It is okay to share your passwords with your parents/guardians though.

Wings Financial Foundation

Test Your Password Knowledge

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

1. L@k3L!f3	Strong	Weak
2. Sam2013	Strong	Weak
3. spike1	Strong	Weak
4. $pR!te#1!	Strong	Weak
5. April152010@	Strong	Weak
6. Luv$2$w!m@1#	Strong	Weak
7. Football#1fan	Strong	Weak

Hint – there are more weak passwords than strong ones!

Briefly explain what makes a strong password:

____

____

____

____

____

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

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