AmeriFirst Bank

Some Information Security Basics

1. Email attachments and links in emails carry the highest risk of infections. Only open an email attachment or click on a link if you're expecting it, know it is legitimate and what it contains. It is best to type the address of a website into a search engine rather than following links embedded in an email.
2. Never click unsubscribe in an email, just send it to Junk and Block Sender.
3. Use a different password for each device/website/software you use.
4. Make sure all passwords are at least 8 characters and made up of at least one number, lower case letter, upper case letter and special character.
5. Never auto save passwords.
6. An email with a zip file attachment is extremely dangerous. An email with an attachment that contains exe should never be opened without checking with IT first.
7. Remember a sign of a Phishing emails is when it asks you to confirm any information or requires you to respond immediately or your account is going to be closed, etc.
8. Do not send any sensitive personal information via email. Unencrypted emails can easily be read by crooks. They can then take the information and use it.
9. To verify a suspicious email, contact the organization directly – but don't call the number or use any contact information provided in the email.
10. Use up-to-date anti-virus, anti-spyware, and anti-adware protection software on your smartphones, tablets and computers.
11. Keep all software up-to-date.
12. Avoid public Wi-Fi is not safe. If you have to use it make sure you software is up-to-date and do not access sensitive accounts (e.g. banks, credit cards, etc.), conduct sensitive transactions over public networks, including hotel and airport Wi-Fi and business centers, or Internet cafés.
13. When you are on the internet do not respond to pop-ups. When a window pops up promising you cash or gift cards for answering a question or taking a survey, close it by pressing Control + F4 for Windows and Command + W for Macs.
14. Ads are very dangerous on websites. It is best to avoid them as they are a popular place for criminals to install malware.
15. Look for "https" when making an online purchase. The "s" in "https" stands for "secure" and indicates that communication with the webpage is encrypted. This helps to ensure your information is transmitted safely to the merchant and no one can spy on it.
16. Never use your work email address when signing up for and accessing personal websites.
17. Use discretion when posting personal information on social media. This information is a treasure-trove to spear phishers who will use it to gain trustworthiness.
18. Do not plug USB cables into public charging stations; only connect USB powered devices using the intended AC power adapter.
19. Don't be fooled by unsolicited calls. The IRS will never call to demand an immediate payment or require you to use a specific payment method. The IRS or any legitimate company will mail you a bill, before contacting you through another medium.
20. When you get a call demanding payment over the phone, hang up and call the company.
21. Shred anything that has your sensitive personal information on it.