APRIL 2020

RETIREMENT CHECK-UP

ANNE ARUNDEL COUNTY PUBLIC SCHOOLS

Managing Your Money (and More) Online… Securely

Managing investments online, as well as paying bills, shopping and banking online, are conveniences that we have all come to expect. They are also services that we trust will be done securely. Multiple layers of security may protect your information online, but it is still important to recognize that you are the first line of defense and the most crucial layer of protection.

Cyber Security

Cyber security is simply the protection of data, programs, networks and computers from unauthorized access that exposes your personal information or uses it in harmful ways.

Our retirement program providers all use high levels of security to ensure that you can view and manage your accounts with confidence. If you haven't already registered your account, do that right now. Your provider will be able to recognize your device and better stop hackers. Of course, it's also a good idea to check your account regularly. Provider websites are:

- Lincoln: lincolnfinancial.com/retirement
- AIG Retirement Services: valic.com
- Voya: voyaretirementplans.com.

When you are online, here are common schemes you may see and ways to protect yourself and your information.

Phishing

Cyber criminals use phishing, through emails and telephone calls, to attempt to obtain sensitive personal information such as:

- Usernames
- Passwords
- Bank information or
- Credit card details

Scammers might pose as IRS agents, financial institutions or credit card companies. How can you recognize phishing attempts?

1. **Mismatched URLs or Redirects:** Check if the website's URL begins with 'https'. Hackers may include a link to a website within the email.

   DO: Hover over the link to see the address. If you want to go to the site, copy the address and paste into your browser.

   DON'T: Click on a link within the email.

2. **Emails conveying a sense of urgency** – for example, your bank account or credit card account has been closed – or emails with supposed information regarding suspicious activity on your account and may be sent with a message asking you to change your password.

   DO: Contact your bank or credit card institution to verify.

   DON'T: Respond to sender and never send personal information or password information via email.

3. **Emails from unknown or known senders that include attachments with no message.**

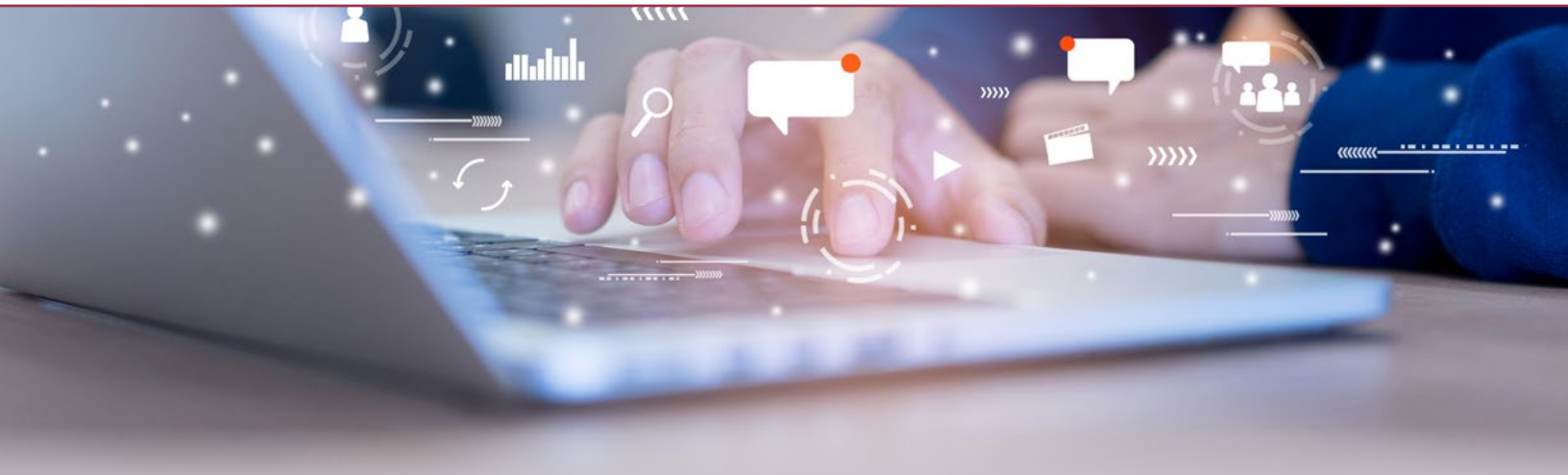
   DO: Delete message and/or mark as spam.

   DON'T: Never open an attachment from an unknown source or sender.

4. **Emails containing very poor spelling or grammar.**

   DO: Anyone can make a typing error so check to ensure you know the sender.

   DON'T: Open or respond to an email from an unknown sender.



Tips to Protect Yourself

Avoid using free, unsecured Wi-Fi for shopping or banking on the Internet and even for logging into your social media profiles.

For social media sites, use an email address that you do not use for important communication.

Use security software with firewall and anti-virus protections and be sure it is up to date.

Don't click on email links or open email attachments from senders you do not know.

Create Strong Passwords. Choose a password that is a mix of uppercase and lowercase letters, numbers, and special characters (symbols). Use different passwords for different accounts (especially those where you have provided your personal information).

Delete old accounts that you no longer use.

Never give out personal information either over the phone or electronically unless you are sure who you are speaking to. If you are asked to provide personal information via email, you can independently contact the company directly to verify this request.

Use your primary email address to stay in touch with people you know or are acquainted with.

Never click on links or download attachments in unwanted, unexpected emails, even if such emails look like they are from a known source.

Do not respond to unwanted, unknown or unexpected emails that ask you to download attachments or click on links. Even if such emails seem familiar, call up the sender and verify the situation first.

AACPS and our retirement program providers want you and your information to be cyber safe.