Cyber Safety Tips

INTERNET SAFETY

➢ PASSWORDS & PRIVACY

Use complex passwords (upper and lower case letters, numbers and symbols) that are difficult to guess and avoid sharing your password.

➢ DOWNLOADS

Never download files from unverified sources or senders. Verify the sources of files and third-party applications before downloading.

➢ OPERATING SYSTEMS

Run updates regularly to keep operating systems and installed software current and protect your devices from viruses.

➢ COMMUNICATION

Always have open dialogue with family members about computer use and internet safety. Ensure children recognize risky situations online and know to alert an adult.

Duty. Honor. Commitment.

police.arlingtonva.us

703.558.2222

PROTECTING YOURSELF ON SOCIAL MEDIA

Limit the amount of personal information you post. Do not post information that makes you vulnerable, such as your address, or information about your daily routine or schedule.
The Internet is a public resource. Only post what you are comfortable with anyone seeing.
Be wary of strangers. It is easy for people to misrepresent their identities and motives on the internet. Avoid interacting with people you don't know.
Be skeptical. Don't believe everything you read online. People may post false or misleading information, and not always with malicious intent.
Evaluate your privacy settings. A site's default settings may not offer the level of protection you desire and may change, so review your privacy settings regularly.
Use third-party applications cautiously. Third-party applications may provide entertainment or functionality, but avoid enabling suspicious applications and limit the amount of personal information the application can access.
Use strong passwords. Protect your account with passwords that cannot be easily guessed. If your account is compromised, someone else may be able to access your information.
Read privacy policies. Some sites may share your information with other companies, which may lead to an increase in spam. Always read and understand referral policies.
Keep software up to date. Install software updates regularly, including updates to your web browser. This prevents attackers from taking advantage of known problems or vulnerabilities. When possible, enable automatic updates.
Use anti-virus software. When kept up-to-date, anti-virus software protects your computer against known viruses, and can detect and remove viruses before they do damage.

PROTECTING YOUR CHILD ON SOCIAL MEDIA

Be involved. Consider activities you and your child can work on together. This allows you to monitor your child's computer habits while teaching safety skills.
Set rules and warn about dangers. Set boundaries for internet usage. Make sure your child understands and recognizes suspicious activity and content, including cyber bullying.
Keep you computer in an open area. Keeping the computer in a high traffic area allows for easy monitoring of computer activity and acts as a deterrent to children who engage in risky activities on the computer.
Monitor computer activity. Know what your child is doing on the computer, including what websites they visit and have a sense of who they contact and interact with online.
Consider partitioning your computer into separate accounts. Most operating systems give you the option to create different accounts for each user. Create a separate account with controlled access and privileges for your child to use.
Consider implementing parental controls. Some browsers and internet service providers allow you to block certain websites on your computer, or allow you to restrict access to those with a password.

More information about cyber safety is available on the Arlington County Police Department's website on the Crime Prevention & Safety page (police.arlingtonva.us/prevention-safety).