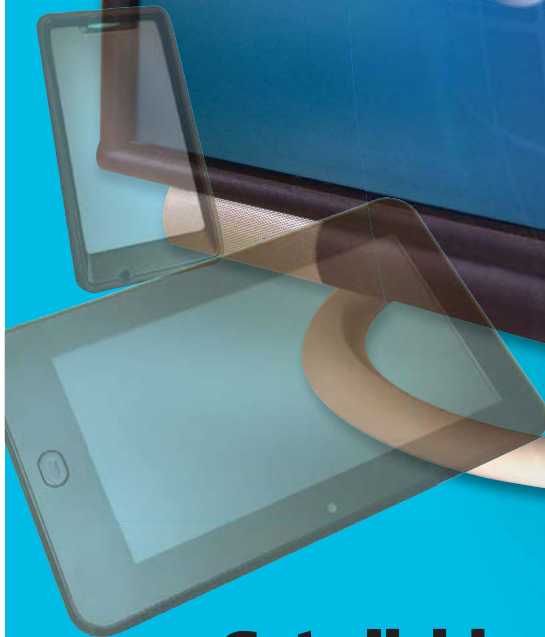




Phishing Hooks



Get clicking! *Don't take the bait. Avoid phishing schemes.*

Cybercriminals lure unsuspecting victims by pretending to be legitimate businesses or friends. They evoke trust to snag personal information or download malicious code, and may make incredible offers or use threats to cloud your judgment.

- Install anti-virus software and keep it updated. Enable it to scan attachments
- Be observant. Ensure that URLs and domain names are spelled correctly.
- Do not enter personal information in a pop-up screen.
- Don't email your personal information.
- Review privacy policies.
- Pay by credit card, not debit card.
- Beware .zip files that may contain malicious files and .doc and .pdf files that could have malicious code embedded.
- When in doubt, don't click links or attachments.

Together we can make a difference!

For more information, visit

www.Chesterfield.gov/cybersecurity



OUR SHARED RESPONSIBILITY