

**HOW TO AVOID
ONLINE SCAMS**

OR

**HOW TO PREVENT
THE GRINCH FROM
STEALING YOUR
CHRISTMAS**

Fords Colony Computer Tech Club
Monday, December 16, 2019



ONLINE/PHONE SCAMS

 Computer Pop-Up Alerts!

 IRS Tax Scam

 Fake Websites

 Grandparent Scam

 Nigerian Scam

 Bitcoin Scam

 Prize Scam

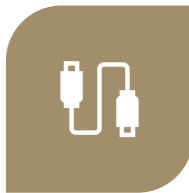
 LOTS MORE...



ONLINE SCAM “HARDWARE” CONTACT POINTS



COMPUTERS/
NOTEBOOKS



USB FLASH DRIVES



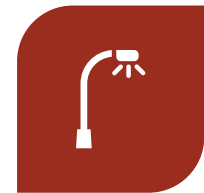
(SMART) PHONES &
TABLETS



WIFI (MAINLY
PUBLIC)



MODEMS/ROUTERS



INTERNET OF THINGS
(IOT) THERMOSTATS,
LIGHTS, SECURITY
CAMERAS,
APPLIANCES



ONLINE SCAM “SOFTWARE/APPLICATION” CONTACT POINTS



EMAIL



SMS TEXT
MESSAGING



PHONE CALLS



INTERNET BROWSERS



WORD DOCUMENTS,
SPREADSHEETS,
PHOTOS, FILES



DOWNLOADING
SOFTWARE FROM
VARIOUS WEBSITES



PRACTICE GOOD COMPUTER/ CYBER HABITS

- 👤 Keep your Software, Hardware, Firmware and Security ***Up to Date***
- 👤 Maintain Strong Passwords
- 👤 Enable Two Factor Authentication
- 👤 Back-Up your Data
- 👤 **Don't Panic, **Remain Calm**** when a computer warning displays



KEEP YOUR SOFTWARE, HARDWARE (*FIRMWARE*) *AND SECURITY UP TO DATE*

👤 Operating Systems-Software:

- 👤 Windows 10 – (version 1909) MacOS – (version 10.15.1 Catalina)
- 👤 Apple IOS – (version 13.3) Android – (version 10.0) (manufacture dependent)

👤 Application-Software:

- 👤 MS Office, Photo Editing, **Antivirus**, Games, etc (Software developer dependent)

👤 Hardware:

- 👤 Computers, Notebooks, Smartphones, Tablets, Routers, Cams, Thermostats etc

👤 Firmware: *(set of instructions programmed on a hardware device)*

- 👤 *Routers, Cams, Thermostats, Computers, Smartphone/Tablets*

👤 Security – Antivirus and Firewall monitoring is always **ON**

👤 Use a Password Manager to create and store your passwords



MAINTAIN STRONG PASSWORDS

- 👤 Make your password long (at least 15 characters)
- 👤 Do not use common phrases or number sequences
- 👤 Use a combination of Upper and Lower Text, Numbers and Symbols
- 👤 Do Not reuse passwords
- 👤 Each of your accounts should have use a different password
- 👤 Strongly Recommend using a Password Manager:

Password managers are programs that allow for the creation and storage of a multitude of passwords.

Examples include: LastPass, Dashlane, 1Password




ENABLE TWO FACTOR AUTHENTICATION

- 👤 When you have to enter only your username and one password, that's a single-factor authentication.
- 👤 Two-factor authentication adds a second level of authentication to an account log-in.
- 👤 Various Two Factor Authentication (2FA) Types:
 - 👤 SMS Text –text message
 - 👤 Authenticator App (examples: Google Authenticator, Microsoft Authenticator)
 - 👤 Push Based – sends a prompt to one of your various devices
 - 👤 Security Key or Card




BACK-UP YOUR DATA *(USE AT LEAST TWO METHODS)*

Cloud Backup

-  Data secured in a remote location. Can set schedule for backup. Can access it anywhere you can reach the internet. Must reach the internet to access your backup files, data transfer speed consideration

External Storage Hard Drive

-  Easy to use, with software, you can schedule backups, Hard disk drives run the risk of failure, Should be stored off-site in case of fire or another catastrophe

USB Flash Drive

-  Portable, affordable, very easy to lose, not always durable

CD, DVD, or Blu-ray Disc

-  Drive failure not an issue, Can store safely in a second location, Legacy technology

Network Attached Storage (NAS) Device

-  Can back up several computers at once, Schedule backups, Expensive, Risk of drive failure



DON'T PANIC, *REMAIN CALM* **WHEN A COMPUTER WARNING DISPLAYS**

🧑‍🚒 **Scammers are great Manipulators**

- 🧑‍🚒 They offer a “free” gift or assistance in (*what we feel is*) a time of need (or emergency!) creating a thankful feeling of obligation towards them.
- 🧑‍🚒 Due to our lack of knowledge and/or being intimidated by the situation (technical issue) and believing that others are being helped in the same way, we play into their hands by making an early commitment to them which lets them takeover the situation
- 🧑‍🚒 *They hold on to us* by being kind, flattering or intimidating and fearful when needed.



RESOURCES TO TURN TO: JAMES CITY COUNTY, VA

<https://www.jamescitycountyva.gov/396/Fraud-Alert>

James City County, VA Report a Scam

If you receive a suspicious call, email, text message, computer/smart phone pop-up or another type of contact that you believe may be a scam or you think you may have been the victim of a scam, **report it to police by calling 757-566-0112. Unsure? Contact Police before providing any personal or financial information.**



RESOURCES TO TURN TO: AARP CONSUMER PROTECTION

<https://www.aarp.org/money/scams-fraud/>

AARP Fraud Watch Network Helpline: 877-908-3360

Our toll-free service is available Monday through Friday, 7 a.m. to 11 p.m. ET

Do you think you have been targeted or have fallen victim to a scam?

Common signs include:

- Receiving a call asking for money or personal information like your Social Security number.
- Finding unauthorized charges on your credit card.
- Getting an email or call saying you've won a sweepstakes or lottery you don't recall entering.

AARP's Fraud Watch Network Helpline, a free resource for AARP members and nonmembers alike, can provide the information you need to protect yourself and your family.



WEB LINKED RESOURCES:

<https://www.aarp.org/money/scams-fraud/info-2019/tech-support.html>

<https://www.aarp.org/money/scams-fraud/info-2017/how-to-handle-tech-support-scams-fd-jj.html>

https://www.treasury.gov/tigta/contact_report_scam.shtml

<https://www.us-cert.gov/>

<https://www.identitytheft.gov/>

<https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams>

<https://www.ic3.gov/default.aspx>

<https://thewirecutter.com/blog/internet-security-layers/>

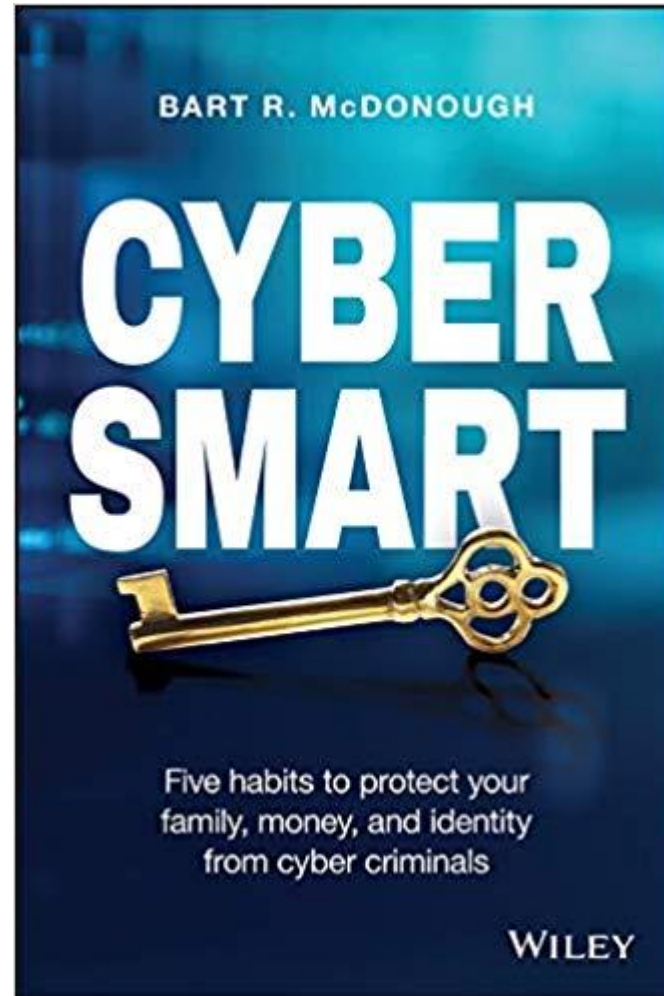


SUMMARY & ADDITIONAL INFORMATION

- 👤 Use of external backup HDD to perform image backups on a scheduled basis; however, ensure they are disconnected from system between backups
- 👤 Use of offsite, online image backup services like Backblaze and others - these provide user a complete image backup should their system be corrupted
- 👤 Use of VPN (Virtual Private Network) when using Wi-Fi other than at home; on computers and mobile devices
- 👤 Use of password managers that require different passwords for each and every site/app - 1Password is one of these APPs; and platform agnostic
- 👤 Use of Bitlocker and equivalents to encrypt everything on your computer systems
- 👤 Malware preventive and detection applications like MalwareBytes; also on mobile devices
- 👤 Ensuring use of router firewalls at point of connection to the internet
- 👤 Also periodically check for firmware updates for routers and Wi-Fi devices, install to keep them up to date
- 👤 Use of limited access to home WiFi for guests; prohibits access to other devices on the local network
- 👤 Use of non-admin account for day to day of computer use; only use admin login only to install, update and delete s/w
- 👤 Create guest (non-admin) account on computer(s) for guest use
- 👤 Use of ad blocking internet browsers vs. Edge, Chrome, Safari, etc.- my current favorite is Brave Browser



SUGGESTED READING:



<https://bartmcd.com/>



?????QUESTIONS?????

