



Tuesday Tech Talk
Computer Security – Steve Nelson
June 16, 2020

LAN: change router admin password/userid, WPA/WPA2, hide SSID? (service set, wifi net name), turn off remote access.

Wifi access physically centered in house, 2.4G v. 5G

Signing On:

passwords, the complex they are, the more complicated they are to hack.

password savers

write them in a note book. secure, accessible. cons, keeping updated.

two factor authentication, if not for everything at least for banking and finances

don't login as admin for everyday use on PC

Microsoft's releases, updates/upgrades, using customers as final test bed

click the Pause button in Windows Update.

saying "no" to pop-ups and phone calls is never wrong

tech support scams, if they're out of the blue they're scams

Resources:

Avoid suspicious links (know the source), Avoid reusing any passwords, get a VPN app for your mobile device, Backup your data to the cloud FOR phones and tables, Enable remote wiping of your phone

get comfortable with web searches, grandchildren and children, AHA requests

what about remote accessing for troubleshooting?

Windows 10 Defender v. 3rd party vendors, esp. AVG

Smartphone & tablet security: <https://www.pandasecurity.com/mediacenter/panda-security/mobile-security-tips/>

1) Keep Your Phone Locked 2) Set Secure Passwords 3) Keep Your Device's OS Up-To-Date 4) Connect to Secure Wifi



Tuesday Tech Talk
Computer Security – Steve Nelson
June 16, 2020

5) Beware of Downloads, only download from official sites

When you are downloading apps, be sure to download them from the official app stores and check reviews. Cybercriminals create rogue mobile apps that mimic trusted brands in order to obtain users' confidential information. To avoid this trap, be sure to look at the number of reviews, last update and contact information of the organization.

6) Don't Jailbreak or Root Your Phone

Jailbreaking or rooting your phone is when you unlock your phone and remove the safeguard the manufacturers have put in place so you can access anything you want. It may be tempting to jailbreak or root your phone to access app stores other than the official ones, but this puts you at high risk. The apps on these illegitimate stores have not been vetted and can easily hack into your phone and steal your information.

7) iPhones are encrypted by default, Androids are not

8) as long as you haven't jailbroken your iPhone, iPod touch, or iPad, you should be safe from viruses

Browser comparisons:

The popular choice: Google Chrome

3x more popular than 2nd--Safari

Pros: safe, speedy, compatible, many extensions available

Cons: resource hog if many tabs open, security concern if google user account is connected to Chrome

A safe choice: Mozilla Firefox

Pros: attention to privacy, auto-blocks 3rd party cookies, private browsing mode, uses less CPU,

C or P? own library of extensions

Con: Design/Interface not streamlined

Apple & Windows Defaults: Safari and Edge

Pros: lightweight and fast re: CPU resources

Cons: not as feature rich



Tuesday Tech Talk
Computer Security – Steve Nelson
June 16, 2020

Honorable mention: Tor Browser

Pros: Top rated anonymous browser, randomly routes traffic through global network of servers

Cons: Based on Firefox but without extensions and extras, some webpages misload depending on servers, extended routing can slow response

Dishonorable mention: Internet Explorer. No longer supported. It's old and in the way.

The browser everyone loves to hate. Use it one time only--to download another browser.

Dishonorable mention: Opera

It had a nice, built-in VPN but has been bought by a Chinese company and is not trustworthy