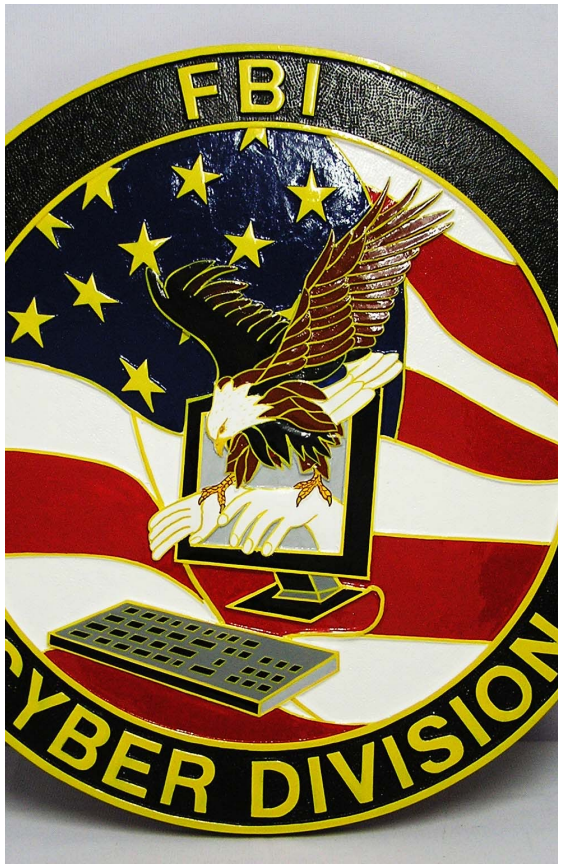
CyberSecurity - How to Protect Home, Work and on the Road

Riverside Financial Group & CMIT Solutions

What we'll cover

Agenda



3 Most Frequent Entry Points

Straight from the FBI, the 3 most frequent ways cyber criminals use

DIY Cyber

What you can do yourself

What to do when it happens

See something, say something – what to do if you see something concerning

Cyber Resources

Resources to learn more about Cyber Resiliency

How they get in

3 Most Frequent Entry Techniques

Educate Yourself!

DIY Cyber Protection

Have an IT Pro to call

- [ ] Password Hygiene
- [ ] OS & Software updates
- [ ] ISP Router isn't secure
- [ ] Next Gen AV
- [ ] Current OS
- [ ] Equipment updates
- [ ] Public Wifi isn't secure
- [ ] Hotel Air BNB not secure
- [ ] Separate work & personal
- [ ] Security Awareness Training – Especially about Phishing
- [ ] Data Backups
- [ ] Vishing / Educate the naive

Password Management is a must.

Password Hygiene

- Long & strong
- Random phrases
- No Reuse
- Password Manager
- KeyChain is safe
- Not in a browser
- Not in a word or Excel doc
- Secure sharing
- Biometrics
- MFA
- SMS Txt not secure
- Howsecureismypassword.net

LastPass

Its not a matter of if but when....

What to do when it happens

- Ransomware
- Phishing email
- Click when you shouldn't have
- Confirm Backups
- Call your IT Pro
- Disconnect from the Internet
- Run a full security Scan
- Disconnect backups
- Change passwords
- Outlook email rules
- Look for extra accounts
- Incident Response Plan

Get Educated

Resources

CMIT Solutions Resource Page – QuickTips, White Papers and more – www.cmitsolutions.com/Stamford/resources

Follow CMIT Solutions of Stamford on Facebook, Instagram, Twitter and LinkedIn

TechCrunch.com

Wired.com

https://resources.infosecinstitute.com/topic/top-9-free-security-training-tools/.com)

www.lastpass.com

Home.Sophos.com

www.cisa.gov/small-business

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics