

Cybersecurity Tips for High Net Worth Individuals and Small Businesses

IERG Webinar Series

February 10, 2016

DR. FREDERICK SCHOLL

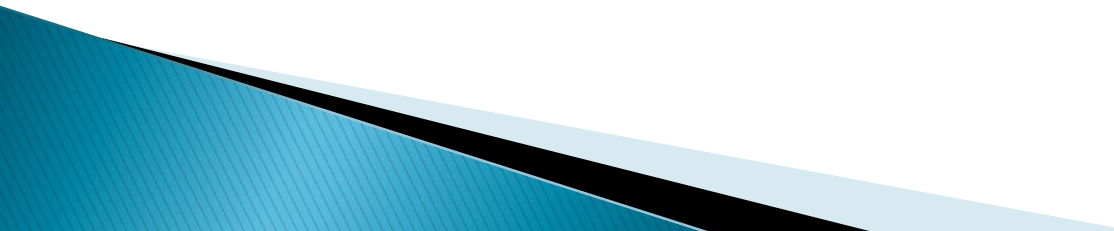
Disclaimers

- ▶ Although I mention certain products...
 - I don't sell any of them
 - There are alternatives
- ▶ You may need a service provider to assist you...
 - I don't provide any of those services either
- ▶ No recommendations can guarantee to keep you secure! Execution is the key!
- ▶ Webinar not endorsed by IRS
- ▶ I am very interested in enterprise security and believe good practice begins at home
- ▶ Cyber threats are global; solutions start at home

Where We Are...

“You’re going to have to be responsible for your safety [in the cyber domain] in a way in which you have not been required to be responsible for your safety [in the physical domain] since the closing of the American frontier in 1980.”

–Gen. Michael Hayden
WSJ, 2/10/2016



Background

- ▶ Tax season is here
- ▶ Tax refund fraud growing at IRS and states
 - \$6.5 billion in 2014
 - 2016: refund fraud could hit \$21B
- ▶ Fraud tied to identity theft
- ▶ DOJ reports 17.7 million cases of identity theft in 2014

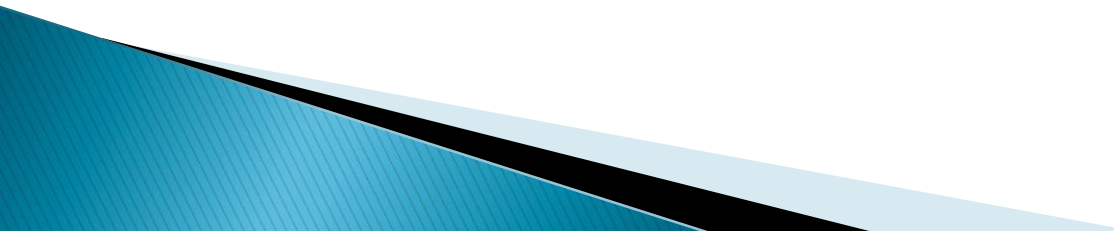
Data is the new currency



Home and SMB Cybersecurity Lagging

- ▶ More and more people work at home
- ▶ Home automation systems growing
- ▶ Home cybersecurity hasn't kept up
- ▶ You have a home alarm system...but not for your network
- ▶ Many people use \$29.95 wireless router to keep secure
 - 7B people can knock on your door
 - 90% have less than \$65,000 in assets

What are the IRS Tax Tips for 2016?

- ▶ Run “deep scan” periodically
 - Windows Defender
 - ESET Smart Security
 - ▶ Better passwords
 - Minimum 8 complex characters
 - 2FA
 - ▶ Tax records on computer should be encrypted
 - ▶ Beware of malware on legitimate sites
 - ▶ Use alerts with credit bureaus, banks and credit cards
 - ▶ Engage kids and seniors
 - ▶ Beware of phishing attacks
- 

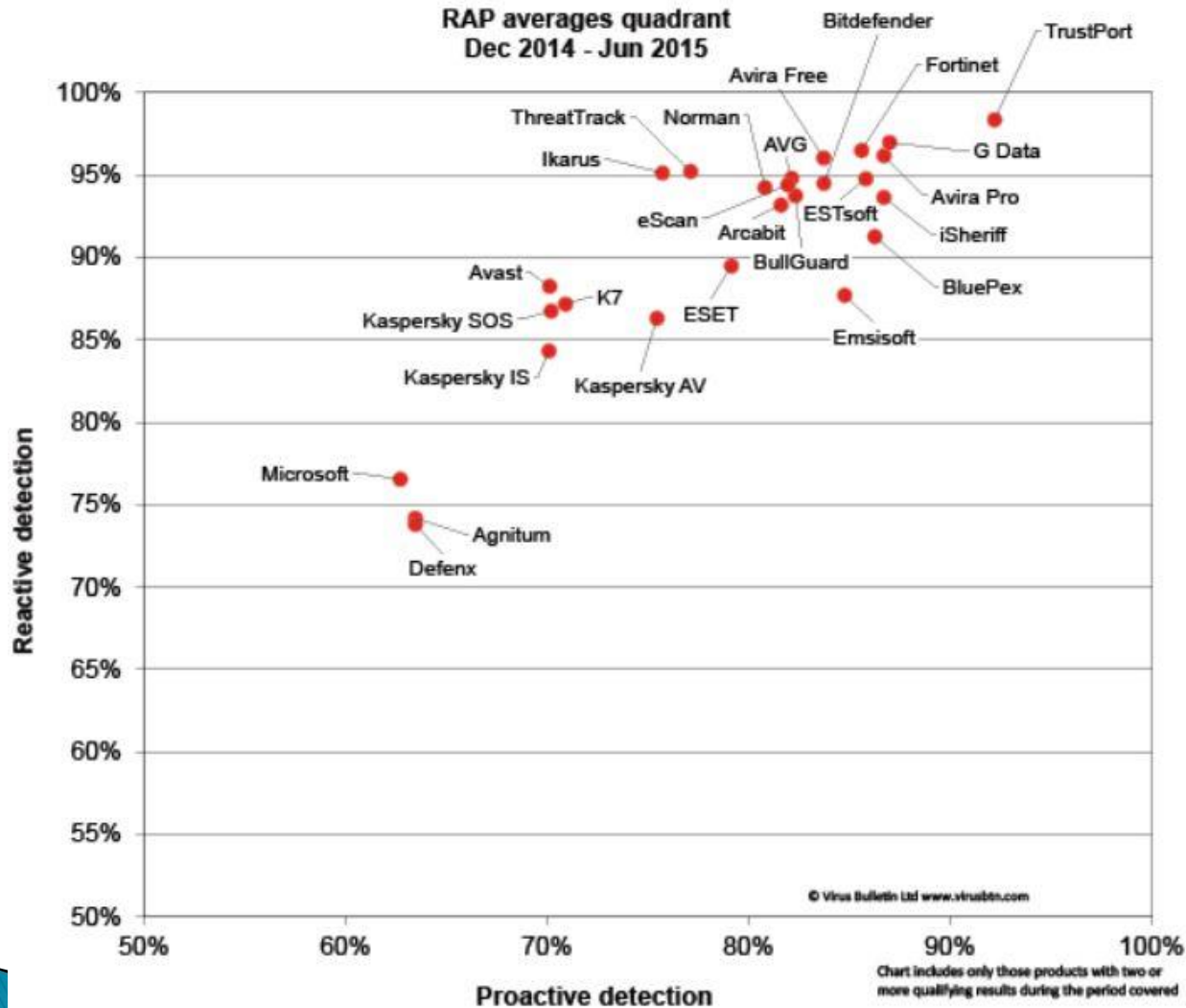
Belt, suspenders and monitoring



No single point of failure



Setting Expectations



Virus Bulletin

Threats and Vulnerabilities

- ▶ FTC says 2015 ID theft up 50% from 2014
 - 490,000 complaints at FTC
- ▶ Tax fraud component growing
- ▶ IRS and states cannot 100% protect you
- ▶ Weaknesses found in home/SMB equipment
- ▶ Good news: capabilities of enterprise security have migrated to home and SMB market...at reasonable cost!
- ▶ You can stay safe at relatively low cost

7 Easy Steps You Can Take

- ▶ Upgrade home router
- ▶ Avoid phishing attacks
- ▶ Don't run as admin user
- ▶ Get rid of data you don't need
- ▶ Have multiple backups
- ▶ Set up a password manager
- ▶ Monitor your financial accounts



Problems With Home Routers

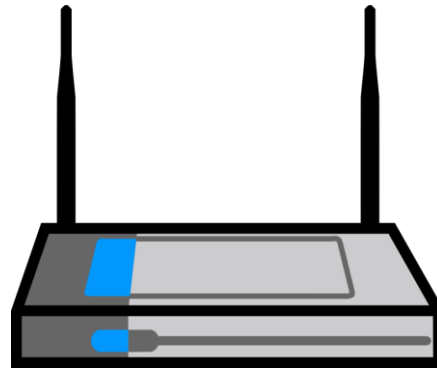
- ▶ Older devices do not have guest networks
- ▶ Difficult to upgrade firmware
- ▶ Vulnerabilities have been identified
- ▶ “80 % of Amazon’s top SOHO routers have security vulnerabilities...34% have documented exploits”¹



Hackers



Website +
Malware



Your Home Router



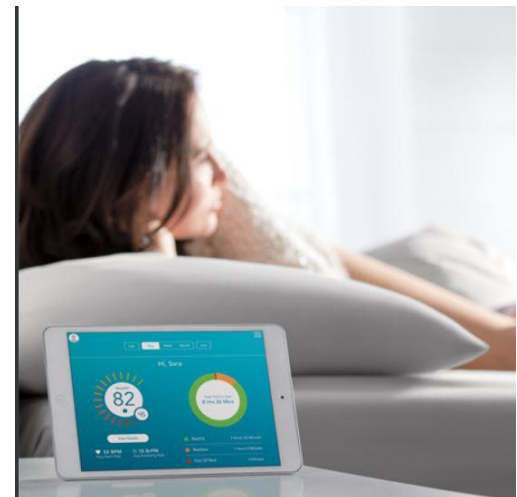
Smart Refrigerator



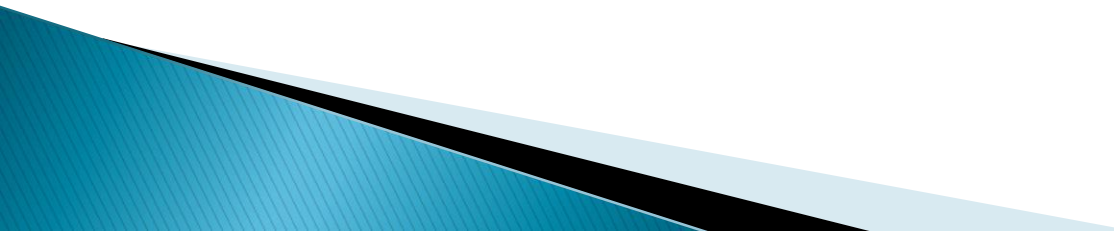
You



Home Visitors



Threats to Home Networks

- ▶ Malware containing web sites that compromise router
 - ▶ Outside attackers that access misconfigured router
 - ▶ Attackers accessing smart home appliances
 - ▶ Visitors or outside wireless network attackers
- 

Current Generation Routers

▶ Security features

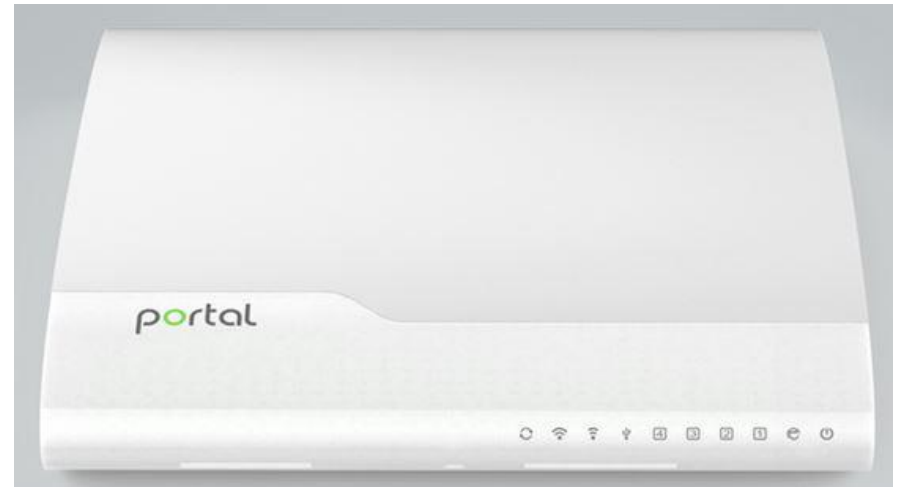
- NAT filtering
- Stateful Packet Inspection (SPI)
- WPA2 security
- Guest network
- Timed access control
- DOS protection

▶ Implementation

- Put your smart home devices, kids and guests on the “guest network”, isolated from your work network
- Update firmware regularly



Next Generation Routers for the Home Market (2016)



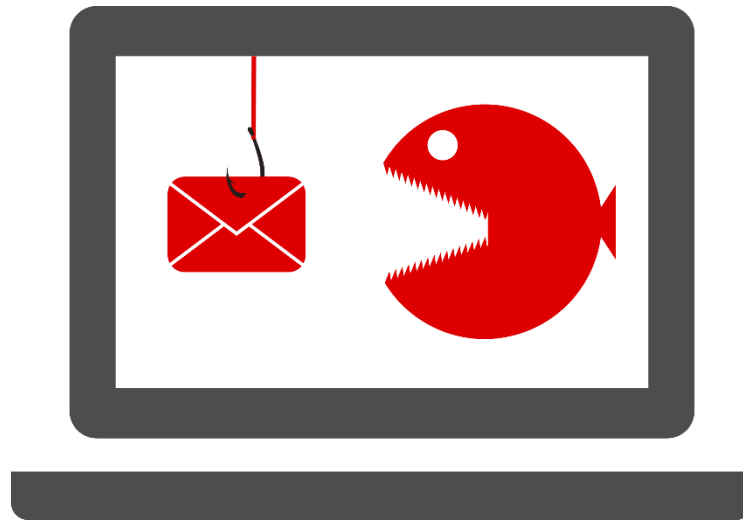
Features:

- Intrusion detection
- Monitoring data exfiltration
- Block unauthorized access
- Cloud based authentication



Avoid Phishing Attacks

- ▶ One of the top “IRS Dirty Dozen” tax scams
- ▶ The most common attack method
- ▶ Not spam, but targeted attack
- ▶ If you are a business executive, you will be a target



Stay Away from Malware Containing Sites

- ▶ Look before you click
- ▶ Browser
- ▶ OpenDNS



Reported Attack Page!

This web page at itsatrap.org has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

[Get me out of here!](#) [Why was this page blocked?](#)

[Ignore](#)

Security

General

- Warn me when sites try to install add-ons
- Block reported attack sites
- Block reported web forgeries

Web Content Filtering

Choose your filtering level

- High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. 26 categories in this group - [View](#) - [Customize](#)
- Moderate** Protects against all adult-related sites and illegal activity. 13 categories in this group - [View](#) - [Customize](#)
- Low** Protects against pornography. 4 categories in this group - [View](#) - [Customize](#)
- None** Nothing blocked.
- Custom** Choose the categories you want to block.

Don't Run as Admin User

- ▶ Switch to admin only as needed
- ▶ 92% of “Critical” Microsoft vulnerabilities can be mitigate by running as standard user
- ▶ Standard user doesn't allow malware installation
- ▶ Standard user doesn't allow malware to defeat AV, etc.



Delete Unneeded Data

- ▶ Paper shredders
 - # sheets per feed
 - # feeds per minute
- ▶ Data shredders
 - Dump old confidential files into Recycle or Trash
 - Overwrite 3–35 passes



Backups and Recovery

- ▶ Need at least three copies
- ▶ Threats
 - Natural disaster
 - Cryptolocker and other ransomware
- ▶ Test how to restore files
- ▶ Dropbox doesn't count as a backup
- ▶ #1 Main
- ▶ #2 Backup drive (Macrium)
- ▶ #3 Cloud (Crashplan)



Using the Cloud or Not?

- ▶ Great for everyday information
- ▶ If you put sensitive data in the cloud you must hold the keys
- ▶ You need client side encryption
- ▶ Dropbox + Boxcryptor
- ▶ Tresorit



Passwords

- ▶ Two password managers needed...
- ▶ File cabinet
- ▶ Online password manager is essential
- ▶ Check your information:
www.haveibeenpwned.com
- ▶ Hacker capabilities (not NSA)
 - 350 billion guesses per second
 - Any strong 8 character password is fair game
- ▶ Password reusing a bad idea!
- ▶ Change passwords regularly

LastPass...|



Monitoring Your Accounts

- ▶ Reactive and proactive
- ▶ Real time monitoring of bank and credit cards
 - Checks over \$XXX
 - Debit charges
 - Etc.
- ▶ Monthly reconciliation, looking for small transactions
- ▶ Credit monitoring: is anyone applying for credit in your name



One More Thing...

- ▶ Patch your software
- ▶ Microsoft released 6 “critical vulnerabilities” yesterday (“patch Tuesday”)
- ▶ Flash player updates again!
- ▶ Chrome browser updates!

Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

[How does automatic updating help me?](#)

Important updates

Check for updates but let me choose whether to download and install them ▼

Contact Information

freds@monarch-info.com

@fwscholl

www.monarch-info.com

Questions & Answers

