Cybersecurity for Regular Folk

Dave Hatter

davehatterlt@gmail.com
www.linkedin.com/in/in/davehatter

March 10th, 2016
Outline

- Threats
- Physical Security
- Email
- Updates/Patches
- Social Media
- Mobile
- Website security
- Data Security /PCI
- Cloud / IoT
- Q&A
Some Eye Opening Statistics

- 2014 has been called the “Year of the Data Breach” and 2015 had 2 less KNOWN breaches than 2014. 2016 is off to a bad start...

- A Champlain college study found:
  - 50% of breaches targeted businesses with < 1000 employees
  - 31% of cyberattacks targeted businesses with < 250 employees
  - 55% of businesses with $10 million or less in revenue reported at least one breach in the 2013. More than 50% of these businesses reported multiple breaches
  - 92% of businesses that were breached lost Personally Identifiable Information (PII) such as credit cards or social security numbers
Some Eye Opening Statistics

- Last year, 594 million people worldwide were victims of online crime. Cybercrime affects millions every year, yet consumers still do not take action to protect themselves.

- Let’s see more:
  - https://us.norton.com/norton-cybersecurity-insights-report-global
For your consideration...

• "There are two kinds of big companies in the United States. There are those who’ve been hacked ... and those who don’t know they’ve been hacked.” – James Comey, FBI Director

• “Techniques, tools, and approaches used to access company networks to commit cybercrime are now available much more widely available along with advice on how to use them.” - Andy Archibald

• For example...
Who cares about my device?

- Any device connected to a network is subject to attack
- There are thousands of worms and viruses that continuously attack indiscriminately
- Hackers may attempt to use your device(s) as zombie or as a stepping stone to launch attacks against other devices
- Hackers and identity thieves want to steal your information and/or money
 Threats

- Identity theft
- Hacking
- Phishing
- Viruses / Malware
- Fraud / Financial theft
- Impersonation
- Information theft
- Reputation damage
Guiding Principals of Security

- Always maintain a healthy dose of skepticism/paranoia!
- Doubt everything & proceed with caution
- If you’re not paying with money, you’re paying with data
- Threats emerge and evolve constantly
- Education and awareness is critical


“Just because I’m paranoid, doesn’t mean they’re not out to get me” – Unknown
Physical Security

- All security starts with physical security
- Control physical access to systems
- Authentication is critical
  - 3 types: password, token, biometrics
  - "What you have, what you know, what you are"
  - Multi-factor authentication
  - Protect credentials as if they are money!
- Password Types:
  - BIOS Passwords
  - OS Passwords
  - Application Passwords
Physical Security

- Lock down systems as much as practical
- Avoid weak passwords:
  - Less than 8 characters
  - Name of family, pets, friends, celebrities, etc.
  - Easily acquirable information such as phone #
  - Common word(s) found in a dictionary
  - Strong password example: 1L0v33mp0e3rU!
- Use a strong, unique password for each site/application/device
- Change passwords regularly
- Password manager app?

http://www.pcmag.com/article2/0,2817,2407168,00.asp
Physical Security

- Biometrics
  - Fingerprint
  - Facial recognition
  - Retinal scan
  - Voice recognition

- Social Engineering
  - Attempt to dupe you into providing info that allows a hacker to access your system(s)
  - Many variants:
    - Phone
    - E-Mail (Phishing)
    - Messaging
    - Social media
You should backup data regularly!

Numerous methods
- External drive
- Flash memory
- Tape
- CD/DVD
- Cloud

Store off-site or in secure location on-site

Consider long-term privacy ramifications
Sanitization

- Data is not physically removed from a disk when deleted
- Common disk utilities such as FDISK and FORMAT will not permanently destroy data
- Tools can retrieve “deleted” data
- “Information leakage” can happen in non-obvious ways. Copiers for example...
Sanitization

- There are essentially 4 ways to permanently destroy data:
  - Physically destroy disk/device
  - Degauss disk with a strong magnet
  - Encrypt data and destroy key
  - Use a disk sanitization tool
    - Norton System Works (www.symantec.com)
    - AutoClave
      (staff.washington.edu/jdlarios/autoclave)
Firewalls

- **Hardware**
  - Router
  - Dedicated

- **Software**
  - Monitor network activity
  - Block ports
  - Notification when your PC attempts Internet access or attempt is made to connect from the Internet
  - Block inbound & outbound access based on rules
  - Scan ports - scan.sygate.com/probe.html

http://www.pcmag.com/article2/0,2817,2369749,00.asp
Firewalls

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

- For your security, some settings are managed by your system administrator.

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

- Domain networks
- Private networks
- Guest or public networks

Networks in public places such as airports or cafés

Windows Firewall state: Off
Incoming connections:
Block all connections to applications that are not on the list of allowed applications
Active public networks:
- Network 3
- SENA-GUEST
- SENA-GUEST
- SENA-GUEST

Notification state:
Notify me when Windows Firewall blocks a new app
Firewalls

ZoneAlarm Free Firewall

Basic Firewall
Blocks invasions and hacker activity
3 access attempts blocked

Alerts and Logs

<table>
<thead>
<tr>
<th>Type</th>
<th>Date and Time</th>
<th>Action</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Co</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:15:24 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.565...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:15:54 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.565...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:25:24 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.565...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:25:52 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.662...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:25:52 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.642...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:45:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.503...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:45:54 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.607...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:55:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.527...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 12:55:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.527...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 13:05:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.575...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 13:05:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.636...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 13:15:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.527...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 13:15:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.568...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
<tr>
<td>Incoming</td>
<td>2016/03/10 13:25:26 -5:00 GMT</td>
<td>Blocked</td>
<td>192.168.134.79.653...</td>
<td>192.168.134.60.7</td>
<td>TCP (flags S)</td>
<td>1</td>
</tr>
</tbody>
</table>
Wi-Fi Security

- Wireless networks are vulnerable
  - Change default password
  - Keep firmware on equipment updated
  - Name network something difficult to guess
  - Don’t broadcast SSID
  - Use Encryption (no open networks):
    - Wired Equivalent Privacy (WEP)
    - Wi-Fi Protected Access (WPA) – better
    - Wi-Fi Protected Access 2 (WPA2-PSK) – best
      - Devices made after 2006 with a “Wi-Fi” logo must support WPA2 encryption
Wi-Fi Security

- **Wireless networks are vulnerable**
  - Only allow known MAC addresses
  - Disable DHCP and use static IP’s
  - Don’t use default subnet
  - Whitelist devices
  - Create a guest network that is constrained
  - Check access logs occasionally for unknown devices
Encryption

- Scrambles data
- Uses complex algorithms to create virtually unbreakable keys
- Data can only be accessed with proper key
- Depending on bit-strength, can be very secure
  - 40-bit is low end, has been broken
  - 256-bit is common now
  - 1024-bit is high-end, virtually unbreakable
Encryption

- Can cause permanent data loss
- Can be cumbersome to distribute and use keys
- Backdoors in products may render encryption moot
Encryption

- **Secure Sockets Layer (SSL)**
  - Web-based
  - Protocol specifier: https://
  - Look for a lock in browser
- **PGP**
  - Phil’s Pretty Good Privacy
  - E-mail
- **Windows supports encryption**
- **Database encryption**
Client Data

- Restrict employee access on a need to know basis
- Audit access to customer information
- Sanitize! Ensure that PII is wiped
- Install regular patches on all components
- The power of Big Data and the Internet of Things (IoT) means ever more data will be collected
Client Data

- Lots of recent high profile attacks
- Personally Identifiable Information (PII)
- More data is collected than ever before
  - Don’t store highly sensitive information if you don’t have to!
  - Password protect customer information
  - Encrypt customer information
  - Keep sensitive customer information disconnected from the Internet
  - Don’t allow employees to put sensitive information on mobile devices
Malware

- Many types:
  - Virus
  - Worm
  - Trojan horse
  - Spyware
  - Adware
  - Bot
  - Zombie
  - Ransomware
  - Rootkit
Malware

- Use anti-malware software such as:
  - McAfee VirusScan
  - Norton AntiVirus
  - Grisoft AVG
  - Trend-Micro PC-cillin
  - Panda Antivirus
  - Windows Defender
  - http://www.pcmag.com/article2/0,2817,2372364,00.asp
Your PC isn't being monitored because the application's service stopped. You should restart it now.

Real-time protection: Off
Virus and spyware definitions: Out of date

Scan options:
- Quick
- Full
- Custom

Start now

Scan details
Last scan: 01/19/16 at 1:07 PM (Quick scan)
Malware

- Beware of file attachments
- Be wary of links
- Stay informed about new viruses and hoaxes
  - US-CERT: www.us-cert.gov/
Malware

- Anti-malware software usage:
  - At least weekly
  - Use auto-update
- Ensure that a full/deep scan is done weekly
- Ensure that all drives are scanned
- Ensure the your software is scanning for memory resident malware
- Consider anti-malware software for your mobile devices
Patches / Updates

- Firmware, operating system and application software undergo constant revisions and improvements.
- Flaws in these complex applications provide hacking opportunities. Eg. Heartbleed.
- Vendors provide “patches” also known as updates that fix issues.
- You must regularly install updates.
- Signup for security e-mails regarding flaws and patches or follow vendors on Facebook / Twitter.
Patches / Updates

Windows Update

Some settings are managed by your organisation.

Windows Update

Updates are available.

- Definition Update for Windows Defender - KB2267602 (Definition 1.215.1053.0).
- Cumulative Update for Windows 10 Version 1511 for x64-based Systems (KB3140768).

Details

Updates are ready to be installed

Install now

Looking for information about the latest updates?
Learn more

Advanced options
E-mail Security

Many Problems with e-mail
- Not originally designed with security in mind
- Malicious payloads
- Threat of information leakage
  - Printing
  - Forwarding
- Violation of privacy
- Spoofing
- Phishing / Spear Phishing
- **Spam**
  - Don’t reply to “get off list”, just delete it unless from a legitimate source
  - Don’t forward mail with list of recipients showing
  - Use Bcc feature for group mailing
  - Don’t post your e-mail address on Web
  - Use a bogus address / change addresses frequently
  - Set e-mail security settings to high (Security tab in Options)
  - Use a Spam filter like SpamKiller
E-mail Security

- Phishing
  - Type of Social engineering attack
  - Much worse than spam
  - Use e-mail to acquire personal information
  - Use spoofed e-mail addresses
  - Emails appear to be from a legitimate source
  - Never give out user name and/or password
  - Check link targets before following link in email
E-mail Security

- Phishing
  - Type of Social engineering attack
  - Much worse than spam
  - Use e-mail to acquire personal information
  - Use spoofed e-mail addresses
  - Emails appear be from a legitimate source
  - Never give out user name and/or password
  - Check link targets before following link in email
  - Spear Phishing: similar, but after money...
New Invoice #3413-1

Portia App <portiaoleh@rambler.ru>

To: David Hatter

This email is being sent in order to inform you that a new invoice has been generated for your account. Please see the attached file.

Thank you.
Portia App
Spear Phishing Example

Joyce Woods
To: David Hatter

Inbox

-----Original Message-----
From: Dave Hatter [mailto:dhatter@fortwright.com]
Sent: Wednesday, March 02, 2016 3:00 PM
To: Joyce Woods <jwoods@fortwright.com>
Subject: Question

Thanks for the information. I need you to initiate 2 wire transfers today for an international payment and a local payment also. Let me know what information is required.

Sent from my iPhone

Sorry Dave,

I just got your message. I have been working on other things. If you mean the General Fund Checking Acct, the balance today is $4,208.49.

Joyce

From: Dave Hatter [mailto:dhatter@fortwright.com]
Sent: Wednesday, March 02, 2016 2:35 PM
To: Joyce Woods <jwoods@fortwright.com>
Subject: Question

Are you available? I need to ask you a quick question. What is the present balance in the operating checking account? Reply as soon as possible.

Sent from my iPhone

Joyce Woods
To: David Hatter

From: Dave Hatter [mailto:dhatter@fortwright.com]
Sent: Wednesday, March 02, 2016 12:35 PM
To: Joyce Woods <jwoods@fortwright.com>
Subject: Question

Are you available? I need to ask you a quick question. What is the present balance in the operating checking account? Reply as soon as possible.

Sent from my iPhone
Messaging Security

- Think Skype or Messenger
- Messaging opens a channel to your device
- Great way to communicate real-time with colleagues
- Can be used to transfer files which contain “malware”
- Can be used for Phishing & Malvertising
- Need to evaluate risk versus benefits
- Must keep client software updated
Web Browser Security

- Enable Security features in your browser
  - Keep browser software updated (patches)
  - Disable cookies, or at least prompt
  - Disable JavaScript
  - Disable Java applets
  - Disable Active X
  - Disable plug-ins
  - Block pop-ups
  - Don’t save passwords
  - Don’t auto-fill forms
  - Look for SSL encryption on e-Commerce sites
Web Browser Security

- Use a secure browser
  - A study has found that Chrome is the most secure browser of the top 3 browsers
  - User Browser plug-in to supplement security
  - Consider using Tor
Social Media

- New channels for attack
  - Phishing
  - Malware
  - Social Engineering
  - Identity Theft
  - Malvertising
  - Reputation
Mobile Security

- Mobile devices are increasingly attacked
  - Convergence of functionality in mobile devices
  - “Smart” phones are getting smarter
  - Many people increasingly use these devices
  - Follow same precautions as PC
  - Beware of public Wi-Fi
  - Install updates regularly!
  - Understand privacy implications of PII
  - Implement AV software
  - Keep firmware on device updated
Website Threats

- SQL Injection
- Input validation
- Authentication
- Malware
- Defacement
- Cross-site scripting
- Unauthorized access
- E-Commerce
  - PCI compliance
The Cloud

- **Outsourcing with a new name**
  - IaaS: Infrastructure as a Service
  - PaaS: Platform as a Service
  - SaaS: Software as a Service

- *Could* be more secure...
  - Experts whose business model depends on security
  - Provides a much larger and more attractive target for thieves and hackers
  - Outsource your security
Internet Of Things (IoT)

- Intelligent Internet connected devices create new risks
- Many of these devices were not designed with security in mind
- Can be used as a conduit to attack a network
- Can be used to host malware
- Can be used to spy on you and your organization
- Could be shutdown remotely
- Understand risks/rewards before adding them to your network
Summary

- Always maintain a healthy dose of skepticism/paranoia!
- Doubt everything & proceed with caution
- If you’re not paying with money, you’re paying with data
- Threats emerge and evolve constantly
- Education and awareness is critical
- 100% secure it nearly impossible

“Just because I’m paranoid, doesn’t mean they’re not out to get me” – Unknown
What are you waiting for?

“The perfect is the enemy of the good”
- Voltaire

Start getting secure now!
Outline

- Threats
- Physical Security
- Email
- Updates/Patches
- Social Media
- Mobile
- Website security
- Data Security /PCI
- Cloud / IoT
- Q&A
Resources

- www.mcafee.com
- www.grisoft.com
- www.symantec.com
- www.lavasoft.com
- www.safer-networking.org
- www.zonealarm.com
- www.zonealarm.com
- www.lavasoft.com
- www.webopedia.com
- www.hackerwatch.org
- www.wardrive.net
- www.antiphishing.org/
- www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
- www.microsoft.com/athome/security/email/phishing.msp
- www.idtheftcenter.org/facts.shtml
- windows.microsoft.com/en-us/windows-8/windows-update-faq
- www.ic3.gov/default.aspx
Questions?

Q & A

Dave Hatter

davehatterlt@gmail.com
www.linkedin.com/in/davehatter
www.youtube.com/davidlhatter
www.twitter.com/davehatter

Catch me on Tech Friday on 55KRC at 6:30 a.m.