Welcome
ScrogginsGrear clients
to
Cybersecurity Education Series
Securing Personal Data

Presenter: Ray Cool, CEO
PBSI Technology Solutions
Webinar will begin at 1:00
Welcome ScrogginsGrear clients to Cybersecurity Education Series

Securing Personal Data

Series Goals

• Inform and educate - How to protect our electronic valuables
• Improve knowledge about electronic security
• Provide practical information about what to change and how to do so

Topic Summaries

• Securing Personal Data - Overview today’s topic
• Email Security Practices 2 of 4
• File Encryption & Cloud Security 3 of 4
• Password Management & Public Wi-Fi 4 of 4
Agenda

Securing Personal Data

Fundamentals of securing important electronic information

- Establish protection from the “open” internet
- Secure your PCs, laptops, phones and other wireless devices
- Protect (encrypt) important personal files
- Backup documents automatically
- Learn principles of Secure Behavior
- Know if your protection is working - Online security monitoring
Who is PBSI?

Technology Services provider for hundreds of clients in the tri-state
Experienced – 75% of staff have 10+ years experience w/PBSI
Proactive IT security for healthcare, business and professionals
Why do we need protection

The Internet Today is a Dangerous Place

Increasingly, PCs are being infected with malware that steals passwords and copies data

New key logging and phishing attacks change constantly – Bad guys are motivated and relentless

The victim is typically NOT notified – Key logging malware may be active on millions of PCs

Email Addresses and Passwords Are For Sale

3.1 Billion emails are available for sale on the Darkweb

1.2 Billion of them include exposed, cracked passwords

LinkedIn, Yahoo, Gmail, DocuSign, Adobe, Dropbox, Tumblr, MySpace and 30 others

Just last week – healthcare.gov – Affordable Care Act (ACA) site for healthcare signup

List of biggest breaches can be found at: https://haveibeenpwned.com

Data Breach Dashboard
Protect yourself from the “open” internet

**Firewall**
With proper settings (run “silent”; advanced packet detection technology)

**Wireless**
Free hacker tools can decrypt almost any password given proximity and sufficient time.
Proximity includes nearby cars & houses. Best defense for wireless - use LONG pw (12+)

Secure all PCs & Laptops

**Antivirus**
This is the last line of defense and MUST be in place on ALL PCs & laptops
Do not use free antivirus. All antivirus vendors have non-free versions. What is different?

**Patch Management**
Set all PCs to auto-update all antivirus, Windows, apps & browsers – as real-time as possible
Once security patches are released, hackers begin probing for old versions immediately
If prompted “Do you want to update?” or “Do you want to reboot?” – answer is always YES

**Vulnerability Scanning**
Most antivirus can run a scan
Who is receiving alerts and acting on alerts?

**Software Downloads**
In an organization, software downloads should require manager approval
Highest risks: Screen savers; weather apps; coupon sites; free movies online; music and lyric sites

Secure Phones & Tablets
Use a Passcode on phones & tablets. Do NOT store saved passwords on laptops
Protect (Encrypt) Files “at rest” & During Transmission

What is file encryption and why is it important?

• Encryption is a term describing data that can’t be read without a private “key” (password)
• Encrypted data is garbled so that if opened it can’t be easily read or interpreted
• Encryption security varies based on technology used AND based on length of “key” (the password)
• Long or complex passwords are encouraged. Length is the enemy of hacker decryption software

Encrypt sensitive files “at rest”

• Which files? Any/all that contain Personally Identifiable Information (PII) or Protected Health Info (PHI)
• Protected information includes SS#s, CC#s, DOBs, Account#s, DL#s, PP#s, medical information
• From whom are you protecting info? Future hackers – If hacked, what could they learn & how would you know?

Encrypt sensitive files during transmission (Email) – 3 Choices

• Encrypt the email – Requires purchase of an email encryption tool
• Encrypt attachment(s) - and provide the password to the recipient – using different medium (text or voice)
• Use a secured file sharing portal – like ScrogginsGrear’s ShareFile
Backup Your Documents

Why? Disaster Prevention

- Disasters happen – hardware failures, ransomware attacks, theft, unintended deletions, operating system updates
- Automatic backup is simple – and important – Most backup “disasters” occur due to human timing failure

Options for Backup

- Local backup, cloud backup, or both
- Choose encrypted local backup, using high-level encryption technology – secure from ransom ware
- Cloud backup – stores multiple previous versions of each document – and is VERIFIED daily

Bottom Line ➔ Backup protection is simply very inexpensive insurance!
Other Principles of Secure Behavior

Internet of Things (IoT)  
Change default passwords! – TVs, Printers, Thermostats, Doorbells, Cameras, Appliances, Alexa...

Phones - Don’t answer (and DO block) unknown numbers – particularly if it matches your area code + 3....
  • Called “Vishing” - Microsoft will not call you to see if your computer is running slow

Privacy Settings
  • Set your PC to disable advertising permissions (NOT the default!)
  • Set your PC to block Pop-Ups. Ublockorigin is a useful app.

Avoid unfamiliar sites for free downloads
  • Free music and free movies are not usually “free”
  • Beware fake Download buttons

Important topics covered in upcoming webinars:
  Email – Learn principles of evaluating “dangerous” emails
  File Encryption & Cloud Security – Learn how to protect sensitive emails & files
  Passwords & Public Wi-Fi – Learn password guidelines & how to securely use public Wi-Fi
Demonstration

Online Security Monitoring

Antivirus
Patch Management
Vulnerability Scanning
Risk Intelligence Scanning - finding unprotected data
Online Backup
Summary - Securing Important Data

Secure your Desktops, Laptops & Phones
- Antivirus & Malware protection – auto updated without manual intervention, daily vulnerability scanning
- Desktop Patch Management - Security issues frequently related to un-updated software patches
- Vulnerability Scanning – Every PC should employ a tool that does a vulnerability scan, every night. Understand alerts
- No unapproved downloads on PCs – Malware comes from somewhere..... Downloads are a BIG culprit

Encrypt sensitive information
- Important protection against a successful hacking event

Backup on an automated schedule
- Don’t let lack of knowledge or attention put you at risk. Use an encrypted backup as a ransom ware protection.

Know if your PCs are safe
- Online security monitoring – inexpensive and very worthwhile

Other Security Issues
- Internet of Things – No default passwords – check every device
- Phone calls – never give secure information by phone

Be an active leaner - Encourage every staff member and family member to learn secure behavior
- Training is inexpensive. Mistakes are not.
Upcoming Webinars

Email Security Practices
• Unsolicited vs. Solicited – Be VERY cautious with all unsolicited email. Does anything seem amiss?
• Antenna up! Is there anything unusual about THIS email? (time of day, recipient list, out-of-context)
• Don’t get your news from email - Beware of current events/product releases received via email.
• Careful with Unsubscribe - Unsubscribe ONLY with known, credible email sources

File Encryption & Cloud Security
• Local & Private storage – Encryption is strongly recommended
• Protected Information sent by email – MUST be encrypted

Password Management & Public Wi-Fi Security
• No duplicate passwords. Do NOT store auto-fill passwords on laptops or iPads
• No passwords on Public Wi-Fi – Use cellular instead
Thank you for your attendance – and thank you to our friends at ScrogginsGrear

Handout will be provided ➔ “IT Security Education – Do’s and Don’t if IT Security”

How can PBSI help you? - All new client pricing will be discounted for ScrogginsGrear clients
ScrogginsGrear Discount - 25% for individuals - 10% for organizations

Contact PBSI for free quotes
• Online Security Monitoring - Antivirus, Patch Management, Vulnerability Scans
• Risk Intelligence Scanning
• Online Backup with Ransomware protection
• Concierge Security Services – Your own security advisor for a low fixed fee per year

Cost
• Online Security Monitoring - Antivirus, Patch Management, Vulnerability Scans $3 - $6 /mo for SG clients
• Risk Intelligence Scanning $2 - $3 /mo for SG clients

Webinar Follow-up
Call or email questions, or free quotation (513) 772-2255 itservices@pbsinet.com
Speaker contact Ray Cool, CEO (513) 924-3915 rayc@pbsinet.com

Upcoming Webinars (you can still register – need to register individually for each webinar)
Securing Personal Information today’s topic
Email Security Practices Thursday, Nov 8 1:00 pm
File Encryption & Cloud Security Tuesday, Nov 13 1:00 pm
Password Management & Public Wi-Fi Thursday, Nov 15 1:00 pm