

Data Security Fundamentals

Best Practices for Small CPA Firms



Derek Houseworth

derek@houseworthconsulting.com

(406) 885-4664

Microsoft
Small Business
Specialist

Computer security is critical for...



Regulatory compliance



Reducing legal liability



Credibility with customers



Competitive advantage



Employee productivity



Peace of mind

Physical Security



- Locate servers, external hard drives, routers & network hardware in secure area
- Avoid sharing work computers with home users
- Avoid storing sensitive information on laptops
- Store laptop in trunk of your car when traveling
- Consider accidental damage and theft insurance for mission critical laptops
- USB flash drives deserve extra attention due to small size

Passwords



- 7 character minimum length
- Include upper & lower case letters, digits and punctuation
- No dictionary words
- Change password immediately if you suspect yours has been compromised
- Using the same password all the time is less secure, situation specific passwords better
- Password protect all computer user accounts
- Lock unattended computers (Ctrl+Alt+Del in Windows)

User Account Control (UAC)



- Intended to prevent malicious software from silently making system level changes
- UAC is a standard feature enabled by default in Windows Vista & Windows 7
- UAC requires user authorization before administrator level changes to system are made regardless of account permissions
- Can be customized so that user initiated actions don't require authorization
- UAC annoying, but worthwhile for most users

Microsoft Office Security



- Office 2007 uses different file extensions & icons for files containing macros present (.DOCM vs. .DOCX, .XLSM vs. .XLSX)
- Don't run macros in Office documents unless you know why they're present and they're necessary
- **Trusted Locations** simple way to provide full macro functionality on internally produced documents
- Documents can be secured with passwords & encryption from within Office applications
- Keep applications updated via Windows Update

Data Storage



- Deleting files not the same as erasing them
- Deleted files can frequently be recovered on most storage media
- Erase all storage devices before recycling or donating old computers & cell phones
- Consider using file system encryption (e.g. Windows 7 BitLocker) on laptops & flash drives
- E-mail & web pages can remain on Internet servers almost indefinitely
- Insure that permissions are properly set to protect shared network folders

Firewalls



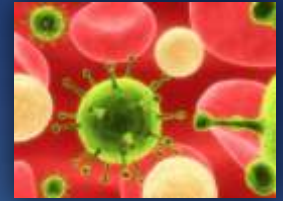
- Purpose is to block unauthorized network traffic
- Firewall on Internet connection is critical 1st line of defense against external threats
- Firewalls can be hardware and / or software
- Software firewalls still valuable, particularly on laptops
- Manual configuration frequently required when some type of connection doesn't work, e.g. remote desktop

Wireless Network Security



- Wired networks more secure & faster than wireless
- Wireless encryption **essential** – use most sophisticated type possible (e.g. WPA/WP2)
- Change router's network name (SSID) and administrative access credentials from factory defaults
- Keep router & firewall firmware current
- Disable SSID broadcast when possible; new computer connections require manual configuration
- Enable **whitelist** of authorized computers if possible
- Avoid transmitting sensitive information over public networks

Malicious Software



- Bogus security software \$150 million industry in 2009
- Threats follow users – Macs not immune, smart phones are new platform being targeted
- Common symptoms of infected computer: numerous pop up ads, unexpected web redirects, slow performance
- Don't be fooled by threatening e-mail messages or websites warning you to “Buy this product, or else...”
- Install legitimate antivirus software on all your computers, particularly in a network environment
- Configure automatic scans and enable them to run regularly
- Keep antivirus program subscriptions current

E-Mail Security



- Don't open attachments, download embedded pictures or click on hyperlinks from un-trusted senders
- Configure junk e-mail (SPAM) filtering at your ISP and/or in your e-mail program (Outlook 2003+)
- Consider viewing all e-mail as plain text in Outlook if SPAM is a problem (**Tools / Trust Center / E-mail Security in Outlook 2007**)
- Opt-out links generally safe way to stop mail from legitimate organizations
- Be aware that Internet e-mail usually not encrypted

Smartphone Security



- Smart phones subject to many of same threats as computers, e.g. viruses, malware
- 10-15% of all handheld devices lost or stolen, employees delay reporting lost devices
- Consider password protection, remote erase, online backup
- Difficult to enforce security & usage policies on personal phones
- Smartphone security threats still emerging

Web Browser Security



- Use most recent version of web browser available (Internet Explorer 8, Firefox 3.6.10, Safari 5, Chrome 5, etc.)
- Install browser updates regularly
- Choose add-ons carefully; mal-ware can be spread via add-on tool bars, games & utilities
- Clear browser cache of files, cookies & history regularly (CTRL+SHIFT+Delete in Internet Explorer)
- Saved password feature can be a risk

Using Cloud Services Securely



- Keep client program current with fixes and updates
- Don't configure programs to save or remember passwords
- Don't access services from potentially infected or compromised computer
- Avoid accessing services over public access networks (e.g. coffee shops, libraries, airports)
- Limit access to service's Control Panel for admin level changes
- Keep your service's tech support contact information on hand

Secure Internet File Transfers



- Encrypted (https) web sites offer secure alternative to e-mail attachments when transferring files
- **MSCPA SecureSend** simple, cost effective way to transfer confidential files
 1. CPA uploads document to secure server & specifies recipient
 2. Secure server notifies recipient via e-mail
 3. Recipient authenticates on secure server
 4. Recipient downloads document via encrypted connection
 5. Secure server notifies CPA transfer is complete
- Potential problems
 1. Recipient doesn't receive notification e-mail
 2. E-mail hyperlinks don't work
 3. Recipient doesn't understand authentication or download process
 4. Document is deleted from server after download

Backup



- Backups must be **regular**, **secure** & **automatic** to properly protect data
- A recent backup should be stored offsite on standard portable media (CD/DVD, flash drive, online or USB hard drive)
- Download speeds limit usefulness of online backup for large volumes of data (e.g. full server restore)
- Role of backup operator must assigned to **trusted** staff member
- Test backup process by periodically restoring & verifying files...don't wait for a crisis
- Backups just part of comprehensive disaster recovery plan

Services Offered by Houseworth Consulting

- Security audits & technology assessments
- IT Support Services
 - hardware & software recommendations
 - computer setup & maintenance
 - helpdesk / tech support
 - network system administration
- Individual & small group training
- Database design & development
- Technology project management



Resources & Tools

- Windows Help
Click Start then Windows Help & Support
- Microsoft Security web site
<http://microsoft.com/security>
- Eraser 6 (free secure file deletion & disk erasing tool)
http://download.cnet.com/Eraser/3000-2092_4-10231814.html?tag=api
- Microsoft Security Essentials - free antivirus program
http://www.microsoft.com/security_essentials
- Microsoft Security Assessment Tool
<http://microsoft.com/downloads>, **search on "Security Assessment Tool"**
- Microsoft Baseline Security Analyzer
<http://technet.microsoft.com/en-us/security/cc184924.aspx>
- MSCPA SecureSend frequently asked questions
<http://www.msccpasecuresend.com/FAQ>
- SBA Disaster Preparedness Planning
<http://preparemybusiness.org>