“When in the doubt, do not click…”

IT Security Briefing

Colt Iseminger

GF Senior Center IT Policy

- Look over the handout
- Keep for your reference

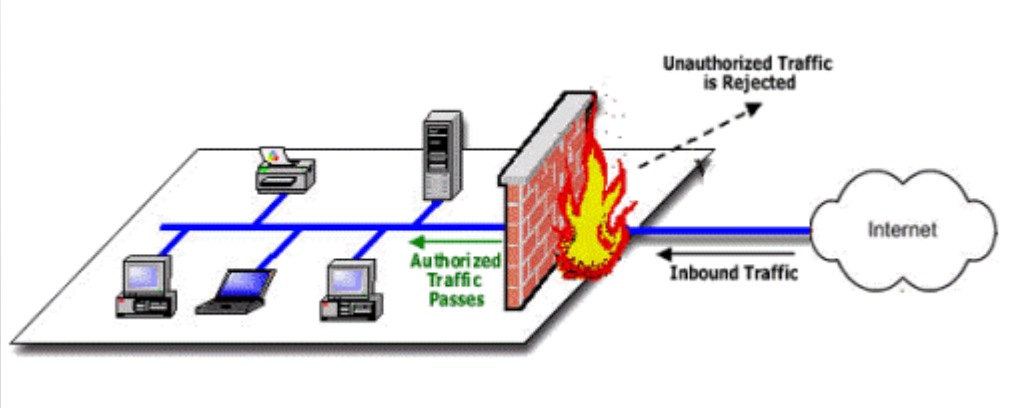
General IT Items

Have a Problem, Restart the Computer

- Estimated 96% of computer problems are solved by restarting the computer.

Firewall – “the Bouncer”

- Firewalls help keep hackers from accessing your computer or network to delete information, to crash your computer, or to steal information without your permission. While antivirus software scans email and files, a firewall is like a guard, watching for outside attempts to access your system and blocking communications from and to sources you don't permit.



Anti-Virus – “the Doctor”

- Antivirus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your computer. Antivirus software works by scanning your computer and your incoming email for viruses, and then deleting them.
- Windows Defender is setup to update and scan automatically.

Passwords – "your Safe"

- Make sure your passwords are strong, are changed periodically, and not the same for multiple services. The longer the password, the better. Consider using a passphrase – a sentence of words (combining with numbers, symbols and uppercase letters makes them even stronger).
- Use a Program to Store Passwords, your "Vault". KeePass is a good program.
- Look for protection for your online accounts beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
  - Example: 2-Factor Authentication (text message code, phone call, etc.)

Passwords should be:

- A minimum of 8 characters.
- A combination of UPPER and lower case letters, numb3r5 and $pec!@l ch@r@cter$.
- Should not be words found in a dictionary.
- Should not be something that is easily discerned from knowledge of the owner.
- Should not be written anywhere.
- Should not sent via email or shared with others.

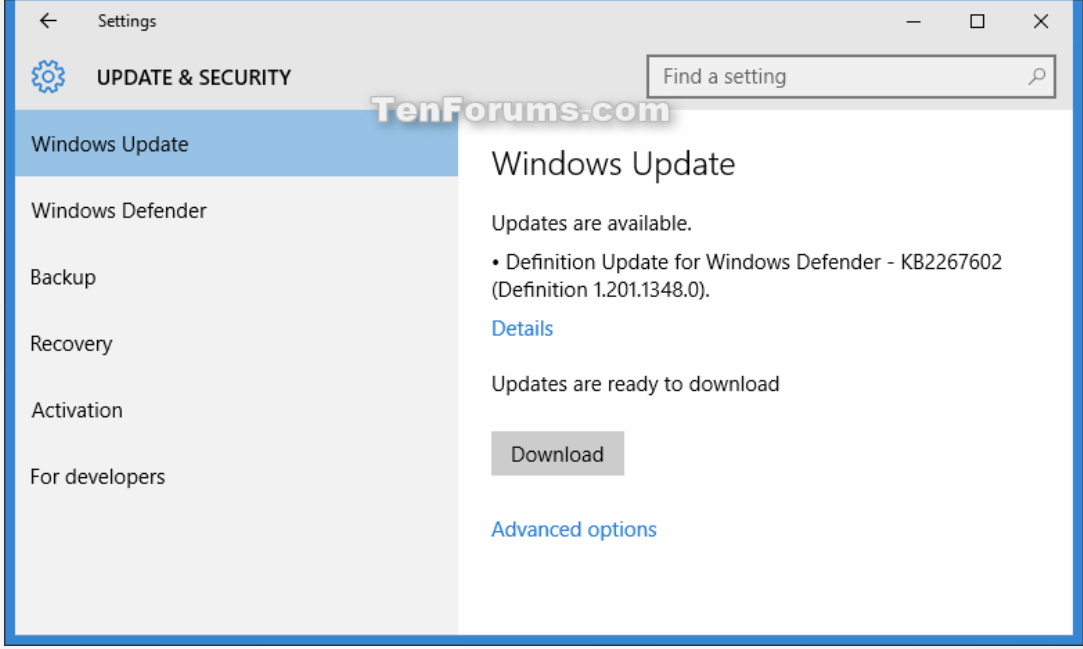
Email

- You should never send sensitive information through email, unless it is encrypted. Email is not a secure transmission method, and this information could be intercepted and read. Also, be suspicious of emails with attachments. Email attachments are a common method to deliver viruses and other malicious programs. If you are not expecting an attachment or the email looks suspicious, check with the sender prior to opening the attachment to make sure it is legitimate, or, even better, just delete the email.

Phishing

- Don't fall prey to phishing attempts. Phishing is when someone sends you an email pretending to be someone you trust and asks you to provide sensitive information, such as a password or credit card number.
- Legitimate emails will never ask for your username and password to be emailed back. Most will not have a web link in them either. They will have you go to your normal website and enter your credentials there.

Software Updates



- Java
- Flash
- Spybot Search and Destroy
- SyncBack
- Windows Updates
  - Operating systems should be set to automatically retrieve and install patches for you.

Vulnerable Programs…

- Apple Quicktime
  - No longer used due to security vulnerabilities with Windows 10
  - Working on Uninstalling on all GFSC Computers
    - Uninstall on your own personal computers also

Recommended Internet Browsers

- Use Google Chrome or Mozilla Firefox
  - Have superior Anti-Malware Protection
- Use Microsoft Internet Explorer or EDGE Browsers only when a site does not work properly on Chrome or Firefox.
  - Example: Harmony SAMS Application

Chrome

Internet Browser Add-Ons Installed on GFSC Computers

- AdBlock Plus – Blocks Ads
- Blur – Blocks Tracking
- Ghostry – Blocks Tracking
- HTTPS Everywhere – try's to force HTTPS connection
- McAfee SiteAdvisor or WebAdvisor – Anti-Malware
- WOT (Web of Trust) – Anti-Malware

HTTPS?

- HyperText Transfer Protocol (HTTP), "S" stands for Secure
  - It is how the Internet sends information from Computer to Server or Server to Computer.
- HTTP is not encrypted and is vulnerable to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information, and modify webpages to inject malware or advertisements. HTTPS is designed to withstand such attacks and is considered secure against them.
- Look for http**s**:// in front of the website address
  - https://www.google.com

Mobile Devices

- Have a passcode/pattern to unlock Smartphone.
- Run Anti-Virus/Malware App
  - Malware for smartphones up 1,800% from 2014 to 2015.
- Only download apps from the Official Android or Apple Stores.
- Be very suspicious of Public Wi-Fi…
  - Everything you do could be watched/intercepted.

Filtering and Data Protection

DNS?

- The Domain Name System (aka DNS) is used to resolve human-readable hostnames into machine-readable IP addresses. This is all done behind the scenes.
- When you type in google.com, our DNS Server Service (OpenDNS.org) returns 8.8.8.8 address for the computer to go to.
- This allows for our Service to "filter" out bad sites, instead of returning the IP address of the site, it returns the site block page.

Grand Forks
SENIOR CENTER
brighter side of sixty

This domain is blocked due to content filtering.

porn.com

Site blocked. porn.com is not allowed on this network.

If you think this shouldn't be blocked, please contact your network administrator.

This site was categorized in: **Pornography, Nudity, Sexuality, Adult Themes, Tasteless**

Diagnostic Info

- [x] Academic Fraud
- [x] Alcohol
- [ ] Automotive
- [ ] Chat
- [x] Drugs
- [ ] File Storage
- [x] Gambling
- [ ] Government
- [ ] Humor
- [x] Lingerie/Bikini
- [ ] News/Media
- [x] P2P/File sharing
- [ ] Podcasts
- [ ] Portals
- [ ] Religious
- [x] Sexuality
- [ ] Sports
- [x] Tobacco
- [ ] Visual Search Engines
- [ ] Webmail
- [x] Adult Themes
- [ ] Anime/Manga/Webcomic
- [ ] Blogs
- [ ] Classifieds
- [ ] Ecommerce/Shopping
- [ ] Financial Institutions
- [ ] Games
- [x] Hate/Discrimination
- [ ] Instant Messaging
- [ ] Movies
- [ ] Non-Profits
- [ ] Parked Domains
- [ ] Politics
- [x] Proxy/Anonymizer
- [ ] Research/Reference
- [ ] Social Networking
- [x] Tasteless
- [ ] Travel
- [x] Weapons
- [x] Adware
- [ ] Auctions
- [ ] Business Services
- [x] Dating
- [ ] Educational Institutions
- [ ] Forums/Message boards
- [ ] German Youth Protection
- [ ] Health and Fitness
- [ ] Jobs/Employment
- [ ] Music
- [x] Nudity
- [ ] Photo Sharing
- [x] Pornography
- [ ] Radio
- [ ] Search Engines
- [ ] Software/Technology
- [ ] Television
- [ ] Video Sharing
- [x] Web Spam

DNS Filtering is not perfect…

- New sites are created daily and may not be included in the filter.
- If you think a site should be blocked that isn't, I need either
  - Website Address
  - Computer, with date and time of the occurrence, with a general idea of the website so I can look it up in History.
- DNS Filtering can not stop direct IP address entry, someone opening files, or email attachments of inappropriate items.

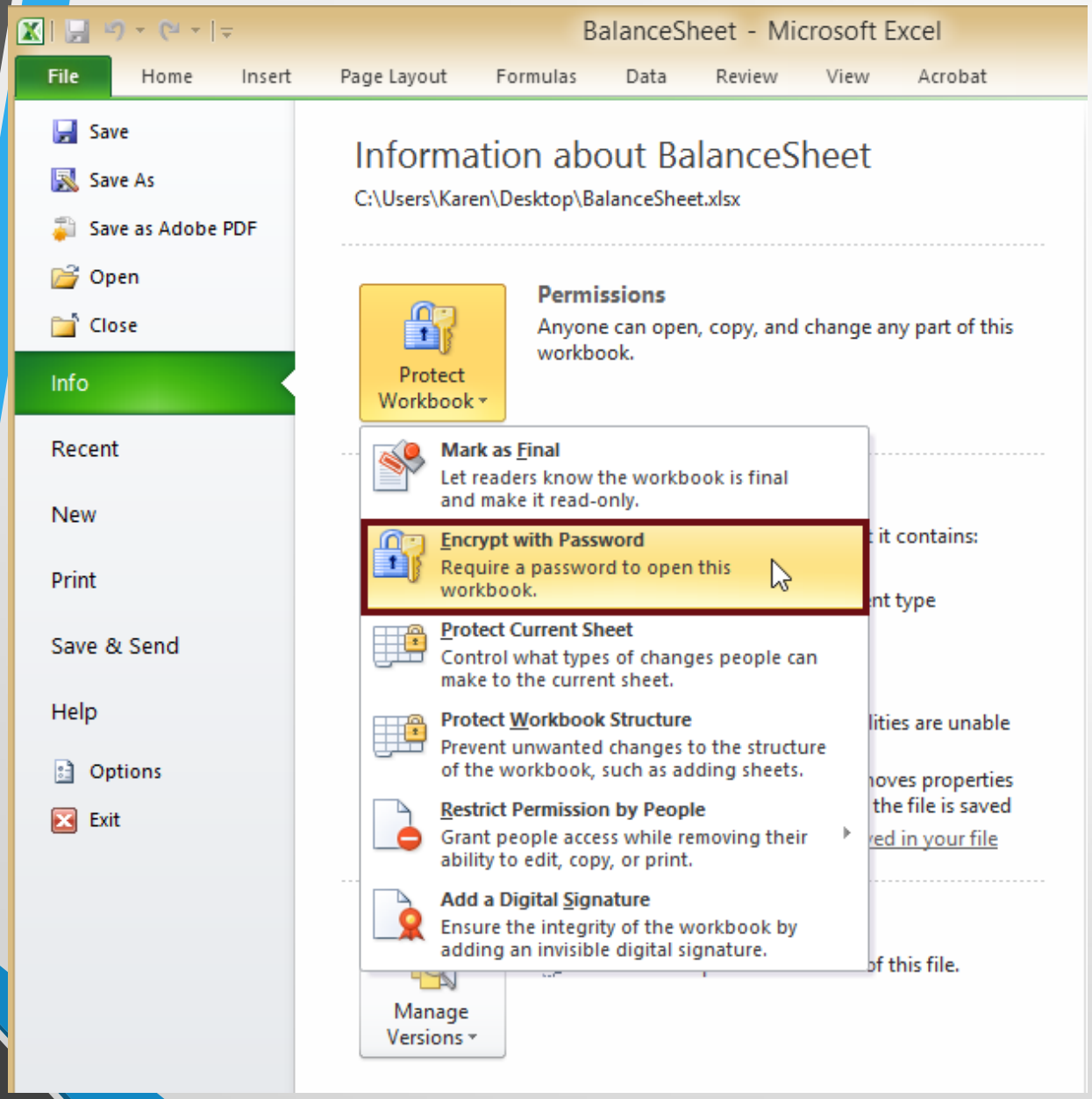
Privacy

- P.I.I. – Personally Identifiable Information. PII can be sensitive or non-sensitive.
  - Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. Non-sensitive PII can be easily gathered from public records, phone books, corporate directories and websites.
  - Sensitive PII is information which, when disclosed, could result in harm to the individual whose privacy has been breached. Sensitive PII should therefore be encrypted in transit and when data is at rest. Such information includes biometric information, medical information, personally identifiable financial information (PIFI) and unique identifiers such as Social Security numbers.
- Physical Paperwork
  - Don't forget about the paper printouts, forms, or other documents you may be saving that have sensitive data on them. Keep them secure and out of public view. When you no longer need them, make sure they are properly shredded or destroyed.

Data Protection

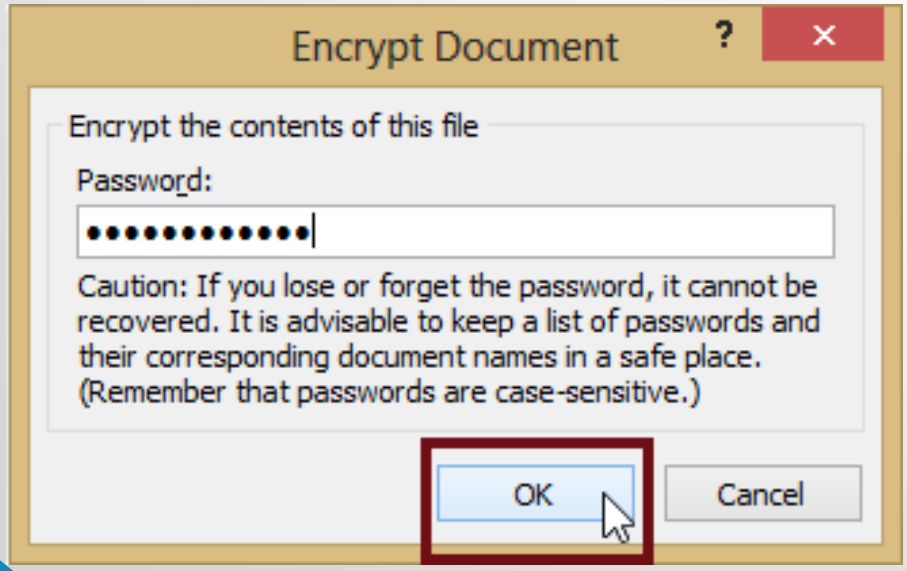
- Stop collecting and storing data unnecessarily. If you don't need to collect and store sensitive information, don't. If you don't really need that information, don't ask for it.
- Storing sensitive data on laptops is especially risky, since laptops are more likely to be lost or stolen. You should also identify and remove all unnecessary files from your computer, especially those files that contain SSN's, credit card numbers, driver's license numbers, or other such confidential information.
- Restrict Access to Sensitive Information

MS Office Encryption



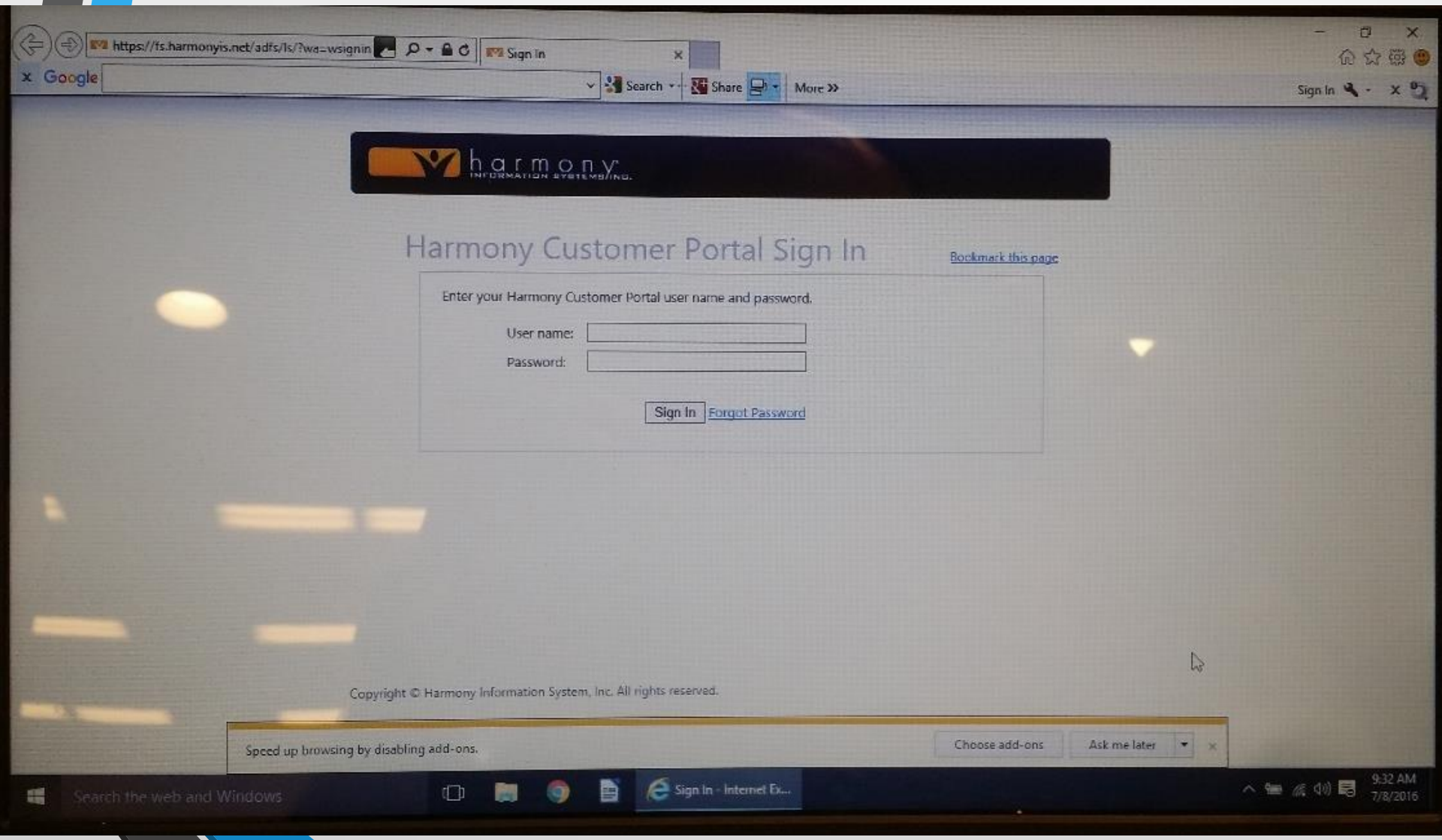
- Password will be required to open the file.
- Click **File > Info > Protect Document or Workbook > Encrypt with Password**

Password Entry and ReEntry



- The Encrypt Document dialog window appears. Type in a strong password and then select **OK**.
- Re-enter your desired password in the Confirm password window and click **OK**.

I.E. Tips


https://fs.harmonyis.net/adfs/ls/?wa=wsignin
Sign In
Google
Search
Share
More »
Sign In
harmony
INFORMATION SYSTEMS, INC.
Harmony Customer Portal Sign In
Bookmark this page
Enter your Harmony Customer Portal user name and password.
User name:
Password:
Sign In
Forgot Password
Copyright © Harmony Information System, Inc. All rights reserved.
Speed up browsing by disabling add-ons.
Choose add-ons
Ask me later
Search the web and Windows
Sign In - Internet Ex...
9:32 AM
7/8/2016

Good Practices

- A “open” wireless connection is less secure than a “secure” wireless connection, which is less secure than a wired connection.
- Use HTTPS whenever possible, when browsing
- Lock Workstation when away from your desk to protect data from Unauthorized Access
  - “Windows Key” + L
- Have a Disclaimer Signature on Emails.

Disclaimer Example from UND

This communication may contain privileged or confidential information and is intended solely for the use of the addressee. You may not directly or indirectly reuse or disclose such information for any purpose other than to provide the services for which you are receiving the information. If you are not the intended recipient, you are strictly prohibited from disclosing, copying, distributing or using any of this information and should contact the sender immediately and destroy all electronic and hard copies of the material.

This message contains information that may be confidential or may contain data that may be subject to the International Traffic in Arms Regulation (ITAR) or the Export Administration Regulation (EAR) of 1979. Regulated data may not be exported, released, or disclosed to foreign nationals inside or outside the United States without obtaining the prior written approval and licenses as required by the U.S. Department of State. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy or disclose to anyone the message or any information contained in the message.

Questions...?