TENISI TECH

MANAGING IT EVOLUTION

Personal Cyber Security Checklist

Sarah Tenisi

CEO TenisiTech

info@TenisiTech.com
408-217-1380

Layer 1 – Your Computer

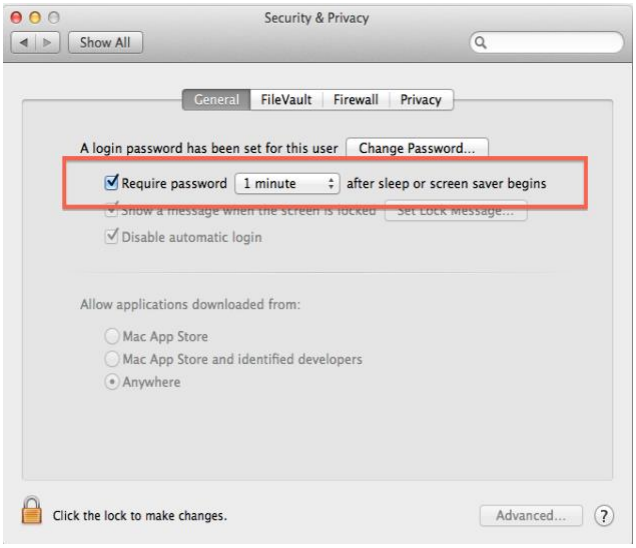
☐ Encrypt Your Computer

Apple Users	Windows Users
Turn on FileVault 2 ☐ FileVault 2 requires OS X Lion or later ☐ Learn How: http://support.apple.com/en-us/HT4790	☐ Check to see if Windows Edition on your computer has the native BitLocker Tool (Windows 10 Pro, Enterprise, & Education) ☐ Right click on My Computer -> Click on Properties

☐ Lock Your Computer

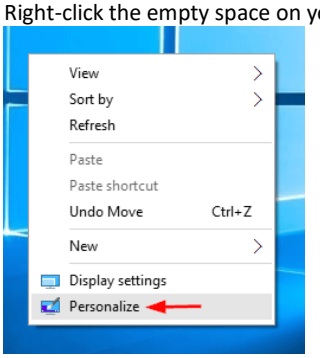
Apple Users

- ☐ Click on Settings -> Security & Privacy
- ☐ General Tab
- ☐ Check Require password
- ☐ Choose a time interval

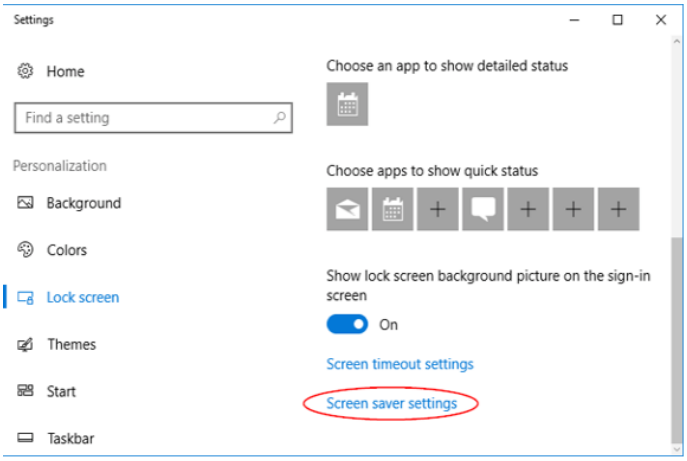


Windows Users

☐ Right-click the empty space on your desktop and select Personalize.



☐ Personalization settings opens. Click on Lock screen in the left pane, then click the Screen saver settings link in the right pane.



info@TenisiTech.com
408-217-1380

☐ Turn on Your Firewall

Apple Users	Windows Users
1. Choose System Preferences from the Apple menu 2. Click Security or Security & Privacy 3. Click the Firewall tab. 4. Unlock the pane by clicking the lock in the lower-left corner and enter the administrator username and password. 5. Click "Turn On Firewall" or "Start" to enable the firewall. 6. Click Advanced to customize the firewall configuration **http://support.apple.com/en-us/HT201642**	1. Open Windows Firewall by clicking the Start button, and then clicking Control Panel. 2. In the left pane, click Turn Windows Firewall on or off 3. Click Turn on Windows Firewall under each network location that you want to help protect, and then click OK. http://windows.microsoft.com/en-us/windows/turn-windows-firewall-on-off#turn-windows-firewall-on-off=windows-7

☐ Keep Your Operating System AND Applications Updated

- Apple users learn how at: **http://support.apple.com/en-us/HT201541**
- Windows users learn how at: **http://windows.microsoft.com/en-us/windows7/install-windows-updates**
- Java (Version 8 Update 25 as of 11/30/14): **https://java.com/en/download/index.jsp**
- Adobe Reader Update:
  - Mac: **http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh**
  - Win: **http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows**
- Flash: **http://get.adobe.com/flashplayer/otherversions/**

☐ Install Anti-Virus Software

- ☐ Check with your ISP (Internet Service Provider) to see if they give you anti-virus software.
- ☐ Use the built-in tools
  - Windows 10 – Windows Defender
  - Mac – Apple builds in various layers of security and you likely don't need anything specific if you keep your OS updated.

Layer 2 - Connecting to the Internet

Home Network	Public Network
☐ Choose a non-standard network name. ☐ Have a password on your network. ☐ Create a separate Guest network. ☐ Turn on your firewall	☐ Use a personal VPN Client

info@TenisiTech.com
408-217-1380

Layer 3 – Your Applications

☐ **Use Two Step or Two Factor Authentication**

Gmail
https://www.google.com/landing/2step/

Apple ID
https://support.apple.com/en-us/HT204152

Microsoft
http://windows.microsoft.com/en-us/windows/two-step-verification-faq

Amazon
https://www.amazon.com/gp/help/customer/display.html?nodeId=201962420

PayPal
https://www.paypal.com/webapps/mpp/security/security-protections

Layer 4 – You

Beware of Phishing

Phishing is defined as: *"The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers."*

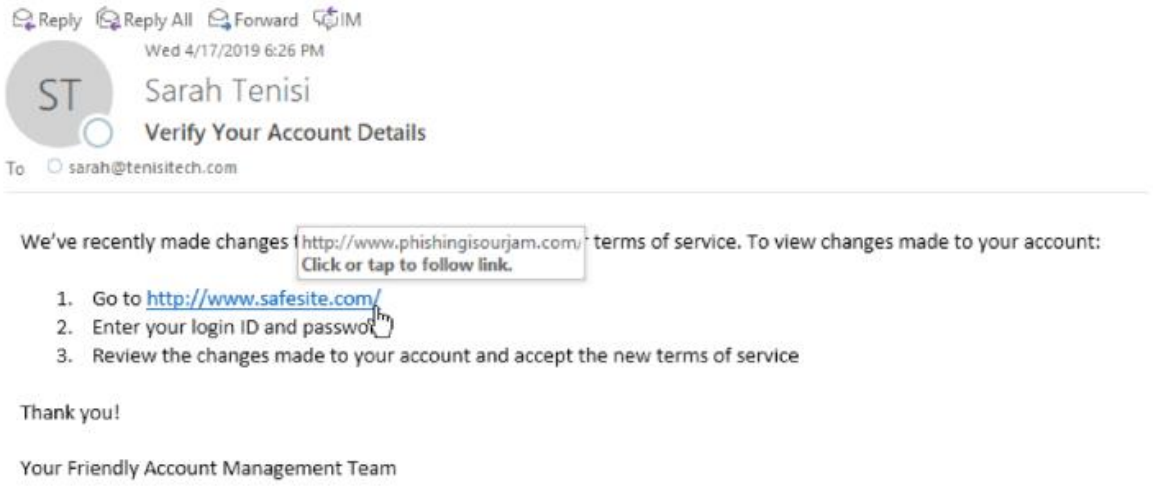
Phishing attacks are very sophisticated and can be easy to fall for. Here are a few essential tips for avoiding phishing attacks

Don't click on links if you do not recognize the sender of a message.

- Check links by hovering your mouse over a link (without clicking!) to see where clicking on it will take you.
- Never enter account IDs or passwords in pop-up windows

Contact colleagues to verify suspicious attachments, requests for money or other sensitive information when in doubt about a message's validity.

In this example below, placing the cursor/hovering (don't click) over the hyperlink, shows that clicking it will take you to a site other than what's shown in the text:



info@TenisiTech.com
408-217-1380

Be Cautious:

- Stop – Read the prompts your computer displays!
- Know your AV software, how it looks and what alerts look like.
- Ensure your family member/others on your computer know your AV tools.
- Verify links by hovering over them BEFORE clicking on them in email messages.

Ask Questions:

Cloud-Related

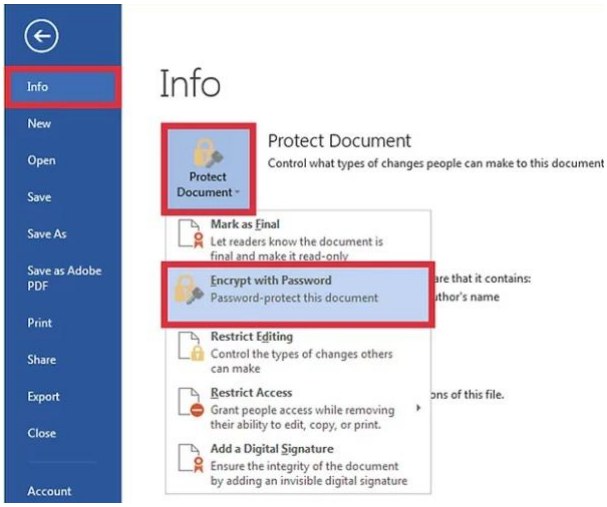
- What type of encryption do you use when transmitting my data?
- Where do you keep my data?
- Who has my data?
- How do I get my data out of your system?

Passwords:

- Use a password keeper
- Choose a strong password (8 or more characters, user upper & lower case letters, numbers and special chars.)
- Don't use the same password for everything, have a few passwords if possible and group sites with a specific password.
- Don't write your passwords down on paper or carry them in your wallet
- Never email passwords.

Password Protect Personal Information in Office Documents:

- In an open document, click File -> Info -> Protect Document and choose Encrypt with Password:



- **Learn how (copy & paste this link into a browser):** https://support.office.com/en-US/Article/Protect-your-document-workbook-or-presentation-with-passwords-permission-and-other-restrictions-05084cc3-300d-4c1a-8416-38d3e37d6826

Mobile Devices

- Set a password on your mobile device.
- Set an automatic lock timeframe on your phone of no more than 15 minutes.
- Ensure that your mobile device and any external storage is encrypted on your mobile device.
- Enable an anti-virus solution on your mobile device.

Know how to "remote wipe" your mobile devices:

- **iOS (Apple) Users –** Learn how:
  - https://www.icloud.com/#find
  - http://support.apple.com/kb/ph2697
- **Android Users** – Learn how:
  - https://support.google.com/accounts/answer/3265955?hl=en
  - http://www.techrepublic.com/article/ring-lock-or-erase-your-lost-or-stolen-android-device/

Send us an email at info@tenisitech.com if you would like this check list in soft copy. Thank you!