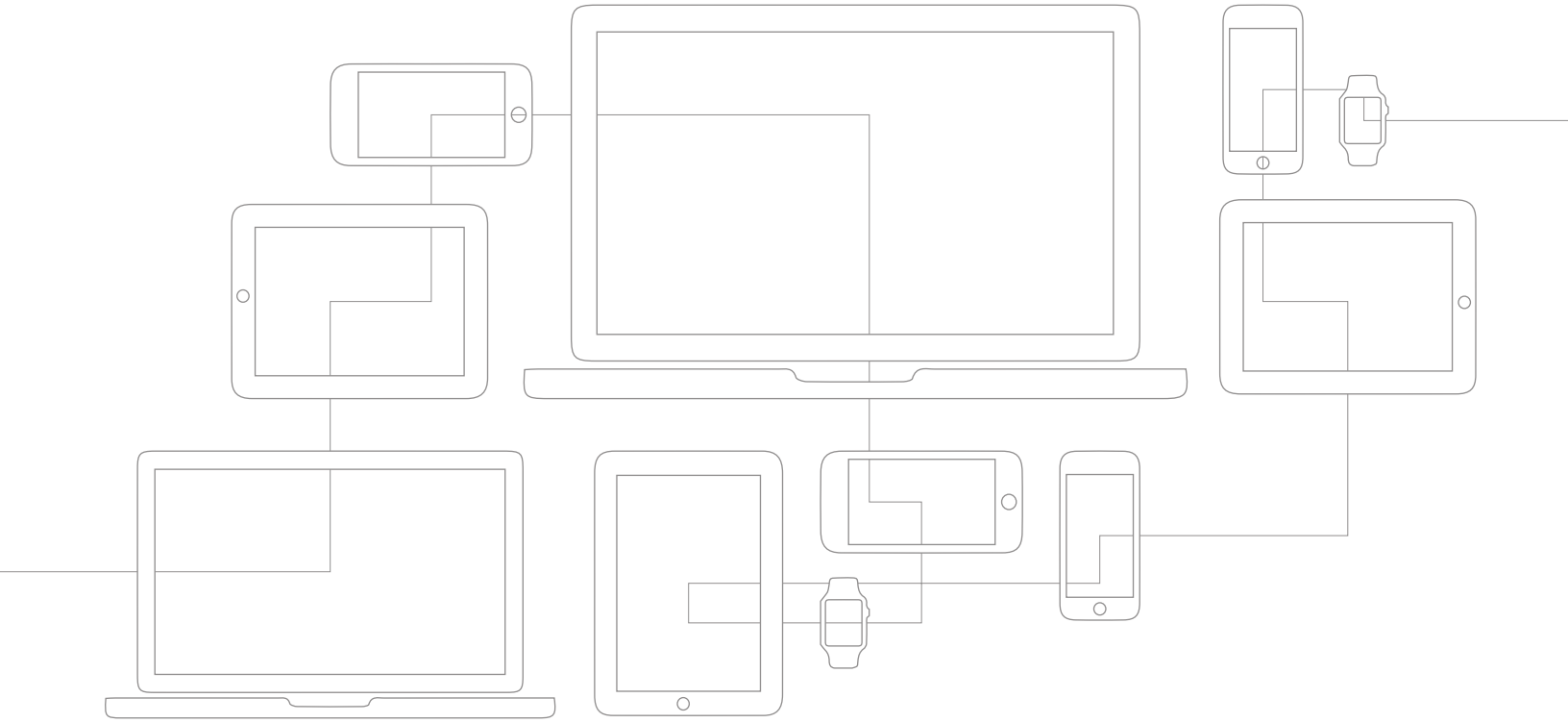
PURE CYBERSAFE℠ SOLUTIONS

Fundamentals Checklist



pure® INSURANCE

		Yes	No	?
01	**Does your computer have an updated version of an antivirus software installed?** All operating systems across both PCs and Macs are vulnerable to viruses and malware. *Recommended:* Install, and keep up-to-date, antivirus software. Never install more than one antivirus as they could conflict with one another.	O	O	O
02	**Do you always update your operating system (OS) and software with the latest patches and releases?** These updates and patches are designed to fix issues with the programs in order to make them run more efficiently and eliminate vulnerabilities that could be exploited. *Recommended:* Regularly check for OS and software updates or configure for automatic updates.	O	O	O
03	**Do you have a firewall enabled and updated on your network (on your router)?** A firewall blocks incoming connections from unauthorized users and software/viruses. *Recommended:* Set up a firewall on your network (typically via your router) and on your laptop (part of your OS). Your Internet Service Provider (ISP) should be able to assist with this.	O	O	O
04	**Have you changed the default password on your router?** If you use the default name and password for your router, anyone within range of your network can see the default name and may be able to find the matching default password by way of an internet search. *Recommended:* Change the name and password on your router. For the name, use something that is not easily identifiable with you/your address. The password should be a minimum of eight characters and should contain numbers, special characters and both upper and lowercase letters.	O	O	O
05	**Do you have WPA2 (WiFi Protected Access) enabled on your Wi-Fi?** WPA2 is the strongest encryption technology available on home networks. It provides stronger Wi-Fi security than other available options. *Recommended:* If the router is provided by your ISP, check with them to see if they can assist; otherwise, check the router manufacturer's website for online guides.	O	O	O
06	**Do you have fewer than 10 individual devices that use your home internet connection (e.g., phones, laptops, dropcam, Nest, TVs, iPads, video game systems, home automation systems)?** Each additional device on a network is another point of vulnerability. Large networks with many different types of devices might benefit from special configurations. *Recommended:* If your network has more than 10 devices connected, you may want to consider a Cyber Risk Consultation.	O	O	O
07	**Do you use a strong, long, unique password for all of the following: laptop/computer login; bank, credit card, and other financial accounts; email accounts?** Strong passwords are a critical defense against cyber attacks. If you use the same password for multiple accounts, when one account is compromised, they all could be. *Recommended:* Each account should have its own password. All passwords should be a minimum of eight characters and should contain numbers, special characters and upper and lowercase letters. Consider a password manager service, such as LastPass or 1Password.	O	O	O
08	**Are your mobile devices Pin Code Lock enabled (and have auto screen lock/timeout)?** If you do not use the lock feature on your phone, the information contained within can easily be accessed should your phone be lost or stolen. *Recommended:* Create a strong password for your mobile device that is easy to remember but hard to guess. Enable your device's auto-lock feature to take effect 5 minutes from the last activity.	O	O	O
09	**Do you use multifactor authentication on email, bank accounts, and all accounts containing sensitive information?** Multifactor authentication refers to the use of multiple points of authentication from independent categories to verify a user's identity. It typically combines "something you know" (most commonly your username and password) with "something you have" (your smartphone) or "something you are" (your fingerprint). When used together, these can greatly increase security. *Recommended:* Activate multifactor authentication on all of your accounts that contain sensitive information. If you have an assistant or accountant who handles financial transactions, work with him/her to establish multifactor authentication protocols so that they are not moving money based solely on an email request.	O	O	O