Protect Your Clients; Protect Yourself

Completing this check list will help you to know the current status and security failures in your business, and the actions you should take to comply with the requirements in Publication 4557 (Rev 6 -2018).

Yes	No	No Sure	No All	How secure is my business?
				I have all my computers running with the latest version of Windows 10 or Windows 8.1 Go to Solution 1
				I have all my computers (workstations, phones*, printers*, servers) protected with Antivirus and Antimalware Protection. Go to Solution 2
				My current Antivirus and Antimalware Protection is updated with the latest virus definition package and include Ransomware and Cybercrime Protection. Go to Solution 2
				My router is upgraded and setup with the latest Wi-Fi secure standards? You share your Wi-Fi with your employees or clients Go to Solution 3
				Do you have network printers, scanner or VoIP Phones? If so...
				… did you change the default passwords? Go to Solution 4
				… do you have the latest firmware and security patches? Go to Solution 4
				Do you have any Data Backup Protection Plan? If so…
				…I have a Local Backup System, and keep monitoring at least every 3 months Go to Solution 5
				…I have an Out-Site Backup System, and I keep monitoring at least every 3 months Go to Solution 5
				…I have a Cloud Base Back System, and I keep monitoring at least every 3 months Go to Solution 5
				…I test my backup system at least twice a year, including hardware testing Go to Solution 5
				At our office, we use an e-mail application like Outlook, Thunderbird, Windows Mail, etc. for accessing our E-mails. Using these tools avoid your employee to expose email password and improve your email security against phishing and spam attacks. Go to Solution 6
				I have the same e-mail and online accounts passwords for the last 6 months or even older? Please change user password with the new guideline's password recommendation, do this at least every 6 months. Go to Solution 7
				I need to trash some old computers, backups, USB memories, external hard drives or printers that could contain sensitive data. Before trash them, you must physically destroy any data storage device before throw away. Go to Solution 8
				I have trained my employees and myself about how identify PHISHING and SCAMS email to protect us from hacker and keep our system secure. Go to Solution 9
				I have trained my employees and myself about how identify SSL SECURE WEBSITES and NON-SECURE OR FAKE WEBSITES. Go to Solution 10
				All the computer at our office are password protected, and I have those passwords in a safe place in case we forgot them or need them. Go to Solution 11
				All my business contact information is updated in my company website, search engine like google, maps, business local directory and social networks like Facebook, twitter. Go to Solution 12
				If your business has a website, or accepts online payments make sure you are using SSL Certificates Go to Solution 13
				We run our antivirus for full scan once in a while, including network and penetration testing Go to Solution 14
				Need more information Go to Solution 15

What's next…

After complete the checklist, please read the solutions below based in your above answers and fix all the issues you could have. Solutions we offer are no final or attached to our services, you can do for yourself all of them, or we can help you, this information is free to share with your employees, friends our partners.

Solution 1

Keep your computer update is the first step to be protected from Virus and Security leaks, if you have any computer running Windows 7, Vista, XP or older, for your security, please upgrade all your computer to the latest Windows version. Microsoft offers a free tool to upgrade to Windows 10, you can do it yourself, a few tips, Backup all your data before upgrade, make sure all your software is compatible with Windows 10, read about how to upgrade your system, and enjoy the new windows. If you have any doubt we can do it for you.

Solution 2

Nowadays, it's very important to have your computer protected, make sure you an antivirus protection, free antivirus are no fully recommended, if you don't have any antivirus or would like to change or upgrade your antivirus, you can find many protection solution in the market, such as: Avast, Panda, ESET, AVG, etc. you can buy any you like, we highly recommend use Antivirus for Business. Some users buy Antivirus for Home because they are cheaper, but remember, you are running a business that require Business-grade protection. We offer this product at www.rimamcs.com/store

Solution 3

In July 2018, a new hack attack breaks out the Wi-Fi security and 90% of router were affected, to fix this issue your router vendor sent a security patch for almost all router, and new security encryption was recommended. Please:

- Make sure your router has the latest firmware version.
- If you shared Wi-Fi connection with your employees or clients, setup a dedicated Guest Wi-Fi, change your password every year is optional but recommended.
- Change default administrative password of your wireless router; use a strong, unique password.
- Reduce the power (wireless range) so you are not broadcasting further than you need. Log into your router to WLAN settings, advanced settings and look for Transmit (TX) power. The lower the number the lower the power.
- Change the name of your router (Service Set Identifier - SSID) to something that is not personally identifying (i.e., MyCompanyTaxService), and disable the SSID broadcast so that it cannot be seen by those who have no need to use your network.
- Use Wi-Fi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption.
- Do not use Wired-Equivalent Privacy (WEP) to connect your computers to the router; WEP is not considered secure.

Solution 4

All network device such, printers, routers, scanner, ip phones, can be accessed using a web browser, make you have changed the defaults password, you can find more information in the device manual section, "how change default password".

Solution 5

Backing up your data is the most important and high priority issue you should take care. As all the solution propose here you are free to choose your products we can help you to setup any of your favorite backup system.
If you need help with your backup system we can help you, we are now offering Cloud-based backup system at www.rimamcs.com/store

Local Backup System, add an external or internal backup disk to backup all your important data, daily, monthly, or yearly.

Out-site Backup System**,** you have to option.

1. Backup your data in an external disk and take this hard disk with you, keep this hard disk in a safe place like your home or any place outside your office
2. Connect and setup a NAS device at your home (or any safe place), and backup your office data remotely using a secure and encrypted internet connection.

Cloud-based Backup System, this is the safer and the only backup solution to protect your data from ransomware and data corruption disaster.

Keep in mind, setup your backup software and forget about it, is no enough to have your data secure, you need to check your backup system at least every 3 months our every time you get an error messages from your backup system, to test your backup: Make sure your backup is running with no errors, the backup software is updates, the hard drive or storage device is not corrupted or has physical damages.

Solution 6

Using email tools like Outlook, Thunderbird, Windows Mail, etc. avoid your employee to expose email password every time they check their email online and improve your email security against phishing and spam attacks.
If you don't have any of these tools, we highly recommend to use them, if you have Microsoft Office in your PC, you can use Outlook our you can user free trusted tool like Thunderbird or Windows Mail, your email provider has information about how setup these tools in their help section under "setup third party mail applications"

Solution 7

It's time to change your emails and online account passwords, Remember:
Use at least 8 character
Use Letters Number and Symbols
Use Upper and Lower Cases
Do not use your name, last name, date of birth, home or business address, or any personal information as your password
Update your Recovery Password information and if Two-Factor Authentication if possible

Solution 8

If you need to trash any old device that may contain sensitive data, before trash them, you must physically destroy any data storage device before throw away. You can your take out the hard drive or usb memory and destroy with a hammer or contact any company the provide this service.

Solution 9

Open the attached file called "IRS p4557.pdf" print and read page 9 and 10

Solution 10

Open the attached file called "IRS p4557.pdf" print and read page 9 and 10

Solution 11

Make sure all your computers have a user password to access, you can do it going to Control Panel, Users, Password and Security. Once you create the password write them down in a save place that will be useful if you forgot them

Solution 12

Search online for your Business, make your all your contact information is updated, update your google listing this will help your clients to find you and avoid phishing attacks.

Solution 13

If you have a website, use SSL Certificates in your site to encrypt all your client data, you can tell you have ssl certificates if your site has httpS (httpSecure).

- Look for the "S" in "HTTPS" connections for Uniform Resource Locator (URL) web addresses. The "S" stands for secure, e.g., https://www.irs.gov.

If you not have a website but you would like to have one, we can help to get everything done, you can read more about at www.rimamcs.com or www.rimamcs.com/store

Solution 14

Run your antivirus full scan and check your system at least once a month, especially during Tax Season, a full scan can take over 2 hours, run the scan after business hours or overnight, if you have a server, check your server updates and test network penetration.

Solution 15

You can find more information in the attached file called "IRS p4557.pdf" or you can contact us for professional advice at:

RIMAM Computer Services
5212 Kester Ave
Sherman Oaks, CA 91411
818 995 6420
info@rimamcs.com
www.rimamcs.com
www.rimamcs.com/store

Most of the above solution can be made by the user without compromising their computers, in any case we, RIMAM Inc, DBA RIMAM Computer Services, recommends create a data backup and basic computer knowledge before proceeding or contact a professional service provider. RIMAM Inc, DBA RIMAM Computer Services, is not responsible for any wrong action our damage you make if you do it yourself. this is for information purposes only