INFORMATION SECURITY BEST PRACTICES

Information security is a challenge for businesses of all sizes. Methods for protecting your computers, business data and your clients' data are increasingly complex and ever changing. No checklist can guarantee security; however, there are some core "best practices" that can minimize many risks to your systems and data. The following "best practices" are recommended for businesses of any size and can also be used in your own personal computer activities at home. If you are uncertain about any of these suggestions, please contact your IT support provider for assistance.

1. Regularly update software

Software vendors regularly provide updates to fix security problems and add or fix functionality. Ensure all software products capable of getting these updates are configured to do so automatically. For those who do not have this functionality, set a calendar reminder to check with the vendor periodically (e.g., once a month) for any new updates. This is the same basic function as having your antivirus software update regularly and automatically, only this is for other software such as the operating system and web browser.

2. Use only maintained software

Using software that is maintained means that the vendor ensures that, as any security flaw or other problem is discovered, a patch is developed and applied. Each revision of software has a useful life, and once that useful life ends, the vendor no longer maintains that software revision, and your systems can be left vulnerable as new weaknesses are exposed and remain unpatched.

3. Change default passwords before using a device/ system for normal "production" activities

Vendor supplied default usernames and passwords are freely and easily available on the internet. These literally are the keys to your systems and data and failing to change these passwords to something only you know leaves your systems vulnerable to easily being reconfigured or accessed without your knowledge.

4. Do not reuse or share passwords

Efforts should be made to use different passwords for each system you access. If your computer login is the same as your customer database, email, bank account and Facebook account, an attacker needs only a single password to access everything. Different passwords will protect against this threat, and software utilities, such as "Password Safe," exist to help manage passwords. You should also never share your password with anyone. Even though the person asking may appear trustworthy, you can't be certain they won't act in a way that may cause your information to be compromised. You also should not be required to share your password in order for any IT or system issue to be resolved.

5. Use passphrases to assist with choosing strong passwords

Complexity typically means having a combination of upper case, lower case, numbers and symbols/special characters and a minimum length. While "Passw0rd!" will typically pass most complexity rules, it is relatively common and easy to guess. As an alternative, consider using passphrases to build a stronger password. A passphrase is generally stronger due to its length, but can be structured to be memorable, which can eliminate the need to write it down. A passphrase is essentially a sentence with some substitution of numbers and symbols for some letters. A "3" for an "e" or an "@" for an "a" as an example, and it might look like IL0v3pysical-Ther@py or P@ssphrases4Life!

PATTERSON® DENTAL

Printed copies of this document are considered uncontrolled. Eaglesoft_Information_Security_Best_Practices
Rev007 | Updated 08.04.2021 22PD289800 (8/21)

6. Be diligent to recognize phishing email attempts

A phishing email is sent by a cybercriminal impersonating an individual or reputable company, in hopes of getting someone to reveal personal information such as passwords or credit card information through links or attachments included in the email. New user credentials are then created, or malware is installed to steal your sensitive data or hold it for ransom. It can be difficult to spot phishing emails, but here are some common red flags to be aware of:

- Misspelled words in the email address or the email domain
- Links or buttons urging you to click within the email have an unknown website address
- Spelling and/or grammatical errors within the email
- Requests to send your sensitive data via email or through an attachment or link in the email

7. Protect your network and computers with a firewall

While a firewall is typically a physical device that sits between the internet and your computers to prevent outsiders from getting to your computers and data, it can also be software on your computer – either included with the operating system or purchased from an alternative vendor. If you have computers that you take home or use at other public locations (hotels, coffee shops, etc.) to perform business functions, ensure that the computer has firewall software installed, enabled and configured.

8. Protect all computers/servers with antivirus and anti-malware software

Install and regularly update antivirus and anti-malware software on every computer (and server) used by your business. Nearly every product in this space can be set to automatically check for and install updates.

9. Secure your wireless (Wi-Fi) network

If you use wireless (Wi-Fi) in your business (or at home), make sure it is encrypted using the strongest encryption settings available to you and your systems. Currently this is WPA-2/WPA-3, but check with your IT support and/or wireless vendors for suggested settings.

10. Do not allow customers to use the same wireless network as your business computers

It is very popular to provide customers with internet access while they are waiting. If you choose to provide this extra customer service, be sure these “guests” are provided an SSID (the name of the wireless network you see when you try to connect), which is different and separate from your business computers and data. In recent years, many vendors have added this feature to their devices.

11. Physically protect business computers and network devices from unauthorized individuals

If someone can physically access your computers and network devices, there is no telling what harm could be done. Ensure your network devices are behind locked doors and only authorized people have access to the room. Further, do not allow computers in public spaces to be left unattended where someone could attempt to install malicious software and/or hardware.

12. Encrypt your data and computing devices

Encryption is critical to protecting sensitive data and can help prevent data loss due to theft or lost devices/media. Further, because encryption protects data, it may help reduce breach notification requirements in many cases. Data that is stored and transmitted should be encrypted. Many software vendors provide encryption capabilities within their products, and a combination of these can provide layers of protection. Configure disk encryption for your computers and servers and configure encryption options for any databases or other key software packages where available.

13. Implement basic security policies

Policies help reinforce the importance of information security – and, depending on the types of data your business handles, may be required. There are hundreds of policies one could devise, but the following may help reduce risks that could lead to a security breach:

- Removable media policy: Restrict the use of USB drives, external hard disks, thumb drives and any other writeable media;
- Password policy: Require unique, strong passwords that must be changed periodically;
- Appropriate use policy: Define appropriate computer and internet use, including that only authorized software may be installed on business computers; and
- Data handling and retention policy: Define how to handle and protect customer information and other vital data; when the data is no longer needed, define appropriate methods for securely disposing of the data.

PATTERSON® DENTAL