PBSI Technology Solutions

www.pbsitech.com

IT Security – Dos and Don'ts of IT Security

My role in keeping important information secure

Avoid downloads and attachments

No software downloads of any kind on my PC unless carefully considered - twice
Includes screen savers – screen savers are frequently the worst security risks
Attachments – Special caution - attachments ending ".exe" or ".zip" or ".bat"

No web links or attachments

DO NOT click on links (or open attachments) in emails – unless you know and trust the source.
Solicited vs. unsolicited email – Avoid clicking on incoming links if unsolicited. Go to web site directly.
Special caution – emails from "known" persons – Check to be sure it is their real email address.
Why? Hacked virus emails frequently come from a NAME you know – with a different email address.
Visit only websites that you have reason to trust - not just a productivity issue – this is a security issue.

Secure my electronic work space

My PC must be set to auto-update current antivirus in as real-time as possible – minimum daily
My PC must be set to auto-update all Windows, apps & browsers
Why? Once security patches are released, hackers begin probing for old versions immediately
If my PC is running slowly – ask for review – don't just assume it is "old"
Slow speed is frequently the result of undesirable software running in background - can be malware.

Keep my passwords private – and unique

Never share my passwords, including wireless passwords – Never ask for others' passwords.
Password security – Never store written passwords anywhere around my desk or keyboard
If my PC displays confidential or protected info, set screensaver on my PC to require a password

External communication of secure Information

Email is not secure – Never email protected information (SS#s, CC#s, DOBs, etc) unless encrypted
If you store secure information (ex: SS#'s, Birthdates) you must not send it via email as text or attachment
Web storage – OneDrive, Google Drive, Dropbox, etc.– Use caution when storing private info w/o encrypted
Social Media – Avoid publishing secure info, including names and birthdates on social sites - Facebook, etc.
No USB drives – Be very careful with backup or portable media (DVDs, Thumb Drives, external hard drives)

No passwords on Public Wi-Fi

Public Wi-Fi is not secure. Unless using a secure app or VPN, do not enter passwords on public Wi-Fi

Document Backup

Document backup is easy and inexpensive – *Please*, don't be overconfident and neglect backup!

Online PC Monitoring

Online PC monitoring is very worthwhile. There is no need to wonder if your data has been compromised.

PBSI -Technology and IT Security Solutions

Modified 1/03/2018