IT Security – Dos and Don'ts of IT Security

My role in keeping important information secure

No software downloads

No software downloads of any kind on my PC unless carefully considered – download from vendor site
Includes screen savers – screen savers are frequently the worst security risks
If my PC displays confidential or protected info, set a screensaver on my PC to require a password

Email Caution! – web links and 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? Malware-laden 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.

Keep my PC up-to-date with all software patches

My PC must be set to auto-update current antivirus in as real-time as possible
My PC must be set to auto-update all Windows, apps & browsers – un-updated patches are a security risk!
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 slow because it is "old".
Slow speed is frequently the result of undesirable software running in background - can be malware.

Keep my passwords private – and unique

Do not reuse passwords. Never use same passwords on work and personal sites. If you have, change them
Password security – Never store written passwords anywhere around my desk or keyboard

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
Cloud – OneDrive, Google Drive, Dropbox, etc.– Use caution when storing private info w/o encryption
Social Media – Avoid publishing secure info, including names and birthdates on social sites - Facebook, etc.

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
Cellular is safe – When in a public place, cellular is always safe. Cellular traffic is always encrypted.

Document Backup

Document backup is easy and inexpensive – *Please*, don't be overconfident and neglect backup!
USB & Backup drives – Be very careful with backups stored on portable media (DVDs, USBs, external drives)

Online PC Monitoring

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