CYBERSECURITY

DO'S AND DON'TS

SECURITY UPDATES

Make certain workstations, peripherals (iPods, iPads, Phones, etc.) are updated with the latest security patches from the vendor.

ANTIVIRUS / FIREWALL

Install, update, and maintain antivirus software and firewall protection on desktops, laptops, and even peripherals where available.

PASSWORDS

First, do not use the same password for everything you work on that is password protected. Second, use stronger passwords that are alphanumeric (e.g. W@t3rm3l0n). Third, do not write down your password on sticky note or otherwise.

BACKUPS

Make certain your data is backed up, and not just once but regularly! Laptops and phones specifically are commonly not backed up and the availability for cloud backups has become so cheap there is no excuse to not backup your data.

ACCESS CONTROL

Make certain you know who is using your devices (desktops, laptops, peripherals) as those people can cause your machine or device to become compromised or data taken.

WIRELESS CONNECTIONS

Make certain not to connect to a public wifi network (i.e. Panera Bread, Starbucks) and conduct any financial or other personal business as hackers or other deviants can monitor and get your information. If you are going to do any personal transactions that include financial, SSN, or health make sure to use a private secure connection (i.e. Verizon Mifi, Home wireless LAN, etc.)

OLD HARDWARE

People throw away hardware all the time and forget to protection your data. Make sure before you dispose of a workstation, peripheral, laptop or otherwise to remove all data from the devices. Any device that stores data, make sure to clear it before you get rid of it!

ENCRYPTION

Encrypt anything that contains sensitive data. Most Operating Systems (OS's) offer encryption and can be used very easily and will save you the hassle later. Just think: if someone were to take your computer, phone or peripheral – what information do they have available to them?

PASSWORD PROTECT

Always use at a minimum, password protection for any device (desktop, laptop, peripheral) to gain access to it. This will provide a basic layer of protection to controlling access to your devices.

EMAIL

Do not open any emails, links, or attachments that are received from unknown sources. This is still the most common way people and companies are compromised using "Phishing" attacks via email.

PRODUCTION
SOLUTIONS™

productionsolutions.com