CYBER SECURITY TIPS

P: (888) 502-3221

Passwords

1. Create passwords that are at least 10-14 characters; use a mix of numbers, upper- and lowercase letters and symbols
2. Change passwords three to four times a year
3. Store in a safe place or utilize a password management tool
4. Do not use the same password for multiple accounts
5. Do not create common passwords
6. Do not select "Remember My Password" on websites you visit

Email

1. Create separate email accounts for work, personal use, alert notifications, and other interests
2. Turn on two-factor authentication whenever an ecommerce site offers it
3. Encrypt important files before emailing them
4. Use spam filtering to stop unwanted email from reaching your inbox
5. Do not open emails from unknown senders
6. Do not reply to requests for financial/personal information

Virus and Malware Protection

1. Keep software/browser/systems up-to-date
2. Install antivirus software and keep it up-to-date
3. Turn on firewall to highest level
4. Regularly back up your data
5. Do not install or use pirated software
6. Do not install P2P file-sharing programs
7. Do not set email to auto-open attachments

Internet Usage

1. Download software only from trusted sources
2. Log out sites instead of simply closing the window
3. Look for https:// for secure session validation
4. Do not click on lonks from unknown/untrustworthy sources
5. Do not allow ecommerce sites to store your credit card information
6. Do not click on pop-up windows to close them; instead use the "X" in the upper right hand corner of the screen

Mobile

1. Keep screen lock on; choose string passwords
2. Select a device with anti-theft features
3. Turn off Bluetooth when it's not needed
4. Regularly update apps (e.g. security patches)
5. Securely back up your data
6. Do not click on ads when surfing the internet

Public Wi-Fi/Hot Spots

1. Disable ad hoc networking
2. Turn off auto connect to non-preferred networks
3. Turn off file sharing
4. Consider using your phone's mobile network instead
5. Do not use/avoid public Wi-Fi
6. Do not use public Wi-Fi to enter personal credentials; your keystrokes can be captured by hackers

Networks

1. Create one network for you and another for guests
2. Change your router's name and password
3. Change the password to your wireless network
4. Turn on your router's WPA2 encryption and firewall
5. Do not use default user names/passwords
6. Do not broadcast personal or business network

Social Engineering

1. Telephone the person who sent the email to confirm its authenticity if you suspect it may be fraudulent
2. Limit the amount of personal information you give out
3. Use privacy settings online whenever possible
4. Do not respond to requests for personal or financial information in an email
5. Do not open an attachment from someone you know if you are not expecting it; call to confirm before opening it
6. Do not assume that every email you receive is authentic

Let us help you with your IT needs.
Give us a call.

Copyright © 2018 InData. All Rights Reserved.