Families First Therapy, LLC

Electronic Security and Safety Tips

Securing your Device

- Have **antivirus, malware, and firewall** both installed, set to automatically scan, and update itself.
- Set up your computer, cell phone, tablet, etc. to **automatically install patches** to the operating system. An unpatched machine is more likely to have software vulnerabilities that can be exploited.
- Enable **auto lock / logoff enabled** on your device so if you step away it automatically locks.
- Setup **full-drive encryption** on cell phones, computers, tablets, etc. with clinical information on them.
- **Securely wipe or destroy** devices when you are getting rid of them.
- **Don't download illegal files** (games, movies, etc); many of these include viruses that will harm your system.
- **Backup** important information regularly (on the "cloud" or an external drive)
- **Don't leave portable technology in a vehicle**. In addition to the attracting theft, heat can damage it.
- **Lock your device** when you aren't using it or when you are away from it.
- Be careful **who you loan your devices to**, even for only a moment.
- Choose a **password** that is at least 10 characters and includes upper/lower case, numbers, & symbols
    - Change it at least every 6 months

Securing your Communications

- Consider using a **VPN** on cell phones, computers, tablets, etc. with clinical information on them.

-- OR –

- Use **secure Wi-Fi networks** for sensitive data transmission (banking, credit card) if you don't have a VPN.

Securing your Email

- **Be warry of giving out confidential, personal, or financial information by email**:
    - A type of digital attack called phishing or scams will commonly do this; credible organizations don't
    - Be careful about links and attachments to emails that look credible; is the sender credible? Many times these links or attachments will have malware, spyware, trojan virus, or other types of attack.
    - Be cautious about unsolicited emails and their attachments.
    - NEVER open an attachment from an email address you don't recognize as legitimate.
- **Don't send sensitive information by email**; it is generally not a secure medium.

Securing your Social Media

- **Limit your social media information** keeping in mind that what's posted may never go away, people you don't intend may see your online content, and some people may try to connect with you online from fictious accounts for the purpose of exploiting your information and contacts.

For more information google "security tips" for most up-to-date information or see this UCLA website:
https://www.it.ucla.edu/security/resources/security-best-practices/top-10-it-security-recommendations

Last Updated: 06.03.2020