The Fulcrum Group, Inc.
Fort Worth 817.697.5043
Dallas 972.695.2304

Free Tips For End User IT Security

It is prevailing knowledge that end users within a business are the weakest link in IT security because they are where the work occurs. The best firewalls, spam filters, and other IT security systems are no match for attacks that completely bypasses all of those IT security measures. Below you will find some free tips for helping end users be more secure, and in turn, tightening the overall IT security of your organization. Knowledge is power!

Before discussing IT security for your small business, executives should make sure their organizations have a solid backup strategy. Make sure you know each of your discrete IT systems, how long you can afford to be down, and how much data you can afford to lose for each system. Don't forget to include data and applications that might be on PCs only or stored in a cloud application. Ransomware and other attacks mean that you need to not only backup your servers, but also your critical workstations.

And here are 10 simple AND free IT security tips that you can provide your end users to make them (and you) more secure.

- **Security Starts with YOU** – Educate yourself about IT security (like reading this document). Know your organization and data. Sensitive data like electronic Protected Health Information (ePHI) in HIPAA and Payment Card Data from PCI have specific legal guidelines to follow. Use common sense (and be suspicious) when dealing with information requests of sensitive information by phone or email – don't be an unwitting victim. Don't put sensitive data on laptops or USB drives that can be lost. Use policies that lock your computer and mobile devices during idle tiles when not in use.

- **Use and Update Antivirus Software** – Even free antivirus software is better than no antivirus software. Make sure that it is set to automatically

update signatures and will perform a scheduled scan at least weekly. Many packages also require you to manually update the base engine (version of the antivirus software). If you suspect you have malware, but your antivirus software doesn't find anything with a scan, run a scan using the free Malwarebytes anti-malware software (valid for personal use only) https://www.malwarebytes.com/business/ .

- **Keep Your Operating System and Applications Updated** – Many security vulnerabilities and attacks can be thwarted simply by keeping your operating system patched and updated. Common desktop applications like Microsoft Office and Adobe Acrobat should be updated as well, as they are common attack vectors. Check out Flexera Personal Software Inspector for a program that identifies updates to your software. http://learn.flexerasoftware.com/SVM-EVAL-Personal-Software-Inspector

- **Disable Java and Flash** – The typical user will rarely have the need for Java and Flash, two of the more common attack vectors used by hackers. If you require, make sure to use the most current version supported by your needed application. https://java.com/en/download/faq/security-tips.xml

- **Avoid Email Phishing Attacks** – Phishing attacks target help from an end user to click a weblink. Never click links in emails or texts that seem to come from your bank, the IRS, or any other institution. Other phishing attack giveaways include poor grammar, misspelled words and offers too good to be true. If you think the message might be valid, open a browser and go directly to the business website to access information., without using the supplied link.

- **Avoid Opening Attachments and Internet Downloads from Untrusted Sources** – Emails can be faked to look like they come from someone you know. Even if you trust the source, think about whether the sender would send you a file and at that particular time. Contact them to verify and be sensitive that attachments and clicking links are main ways ransomware and infection occurs on a business network.

- **Use Passphrases Instead of Passwords** – Short, simple passwords are easily cracked with a dictionary attack and longer, more complex passwords are difficult to remember. Instead, start with a memorable phrase that only means something to you (but don't use birthdays, names of pets, etc.), then add a mixture of upper case letters, symbols or numbers, and you've now got a difficult to crack password that you can actually remember. The sample password "TodayIsMyDay7" with 13 characters and 3 of the 4 character types is probably harder to crack and easier to remember your current password. *Bonus Tip: Change your passwords often, and never use the same password on more than one system or website.*

- **Be Secure with Your Mobile Devices** – Research what apps you choose to install for validity and pay special attention to what permissions each app is requesting. Set your smartphone to lock after a short idle time, and set it to require authentication for unlocking. If at all possible, use something stronger such as six-digit PIN or newer fingerprint capabilities.

- **Avoid Open Wireless Networks** – If you connect to open wireless networks that don't require an encryption password, then much of the data that you send and receive across that network is not encrypted and is insecure. Separate guest networks from your regular users and make sure to use preferred encryption types such as WPA2 over WPA.

- **Social Media Risks** – It's tempting to post on social media while you're away on vacation, but you could be letting thieves know you are away from home. Review your social media privacy settings frequently so that you don't share information with the wrong people. Photos at the office could show technologies in use, passwords on Post-It notes, privileged

documents on the desk or other information you'd prefer hidden. And remember that anything posted on the Internet can remain there forever.

We hope these 10 free tips will quickly help users keep your IT environment more secure, so you can focus on running your business!

Once you're ready to take a more strategic approach, we can get into a discussion about Best Practice standards for IT security in small to medium businesses and organizations. These are systems and processes that every organization should have as a MINIMUM.

- **IT Security Policy** – IT security policy consists of high level statements relating to the protection of information across the business and should be produced by senior management.

- **IT Security Standards** – Standards consist of specific low level mandatory controls that help enforce and support the IT security policy.
- **IT Security Guidelines** – Guidelines consist of recommended controls that help support standards. IT Security Guidelines are offered by organizations such as ISSA, (ISC)2, SANS, and NIST.
- **IT Security Procedures** – Procedures consist of step by step instructions to assist workers in implementing the various policies, standards and guidelines.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Fort Worth phone 817.697.5043 Dallas phone 972.695.2304 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro

- **IT Security Systems** – Layered, "Defense in depth" approach to security:
  - Next Generation Firewall with layers of security (web filtering, network antivirus, intrusion prevention, etc.)
  - Centrally Managed Antivirus for Desktops and Servers
  - Properly segmented wireless networks (ensuring guests can't access your private network)
  - Physically protected server and equipment rooms
  - UPS to keep equipment running during short power fluctuations or outages
  - Backups and Disaster Recovery Systems, well documented and regularly tested
  - Network monitoring to check network and server performance trends
  - Security monitoring to aggregate logs from different systems and make sure attempted attacks are guarded against

Remember: Small Businesses with secure IT environments usually have fewer IT emergencies and can spend more of their IT resources helping transform the business.

THE FULCRUM GROUP
One Technology Solution: Yours

The Fulcrum Group, Inc. 5751 Kroger Drive, Suite 279, Fort Worth, TX 76244
Fort Worth phone 817.697.5043 Dallas phone 972.695.2304 Fax: 817.337.0313 Help Desk: 817.898.1277
info@fulcrumgroup.net www.fulcrum.pro