Securing + Updating Personal Devices

CIA Information Technology (IT) recommends that you enable device passcodes and login passwords on all personal devices and keep personal devices up to date with the latest versions of the software available from the device manufacturer. In order to access CIA on your mobile devices, you will need to enable a passcode.

CIA IT recommends that before you perform any updates to your device, you first back up the device according to manufacturer instructions.

Resources for Enabling Device Passcodes or Logins:	
Mac	https://b.link/gs7jhr
iPhone	https://b.link/58m60r
iPad	https://b.link/plce9m
Windows	https://b.link/9x1z5r
Android	https://b.link/2zxvw6

Resources for Performing Device Updates:	
Mac	https://b.link/qnu14g
iPhone / iPad	https://b.link/187xb3
Windows	https://b.link/o9kllv
Android	https://b.link/k52jy4

Resources for Performing Data Backups:	
Mac	https://b.link/ucy03v
iPhone	https://b.link/grcbmr
iPad	https://b.link/kyablj
Windows	https://b.link/9kddsb
Android	https://b.link/vorptu

12/14/22

For mobile Apple devices (iPhone, and iPad) there is not a third party security software that we recommend at this time.

For Mac, PC and Android, CIA IT recommends the following products. These products range from free-to-use apps to subscriptions for dedicated Antivirus software. Please note that this is not a comprehensive list.

Resources for Security Applications:		
Application	Cost	Resource / Link
Malware Bytes: Anti-Malware	- Free trial for limited use - Paid versions for extended use	https://b.link/jxxmx6
Norton 360 Deluxe: Anti-Virus	- Paid subscription is available to CIA faculty, staff, and students at a significant discount through On The Hub.	https://b.link/5au7q6

** Please note that CIA Information Technology will not support and is not responsible for your personal device or data, and we cannot be held responsible for any loss or damage to your device or data as the result of following any of the above recommendations or use of any of the above products**

If you have any questions, please contact CIA IT using the support form at: support.cia.edu.

Cybersecurity Skeptic No More!

I help protect my organization from cybercrime by keeping these tips in mind, and you can too!

Phishing Emails | Identify phishing emails

- Does the email come from an unknown sender, or is the email address misspelled?
- Does the email contain grammatical errors and misspelled words that are unusual from the sender?
- Does the message create a sense of urgency, such as stating that immediate action is required?
- Does the email include unexpected attachments or suspicious links?

Account Protection | Create strong passwords

- Create a memorable, complex password with at least 16-20 characters.
- Never reuse a password.
- Use an organization-approved password manager.

Websites and Links | Avoid clicking on malicious links

- Review them carefully. Cybercriminals may disguise, misspell, or add extra characters to the link to look like a trusted website.
- Search for the website's actual domain using a search engine like Google or Bing. When in doubt, don't click on the link.

Cybercriminals can target anyone, even you! If something seems suspicious, report it!
Remember these tips to protect yourself and your organization!

KnowBe4