African Cyber Security

BEST PRACTICE GUIDELINES FOR CONSUMERS

Protect Yourself

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file- and heuristic-based) and behavioral malware prevention can prevent unknown malicious threats from executing.
- Bi-directional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer.
- Browser protection will protect against obfuscated web-based attacks.
- Use reputation-based tools that check the reputation and trust of a file and website before downloading, and that check URL reputations and provide safety ratings for websites found through search engines.
- Consider options for implementing cross-platform parental controls, such as Norton Online Family.

Update Regularly

Keep your system, program, and virus definitions up-to-date; always accept updates requested by the vendor.

Running out-of-date versions can put you at risk from being exploited by web-based attacks. Only download updates from vendor sites directly. Select automatic updates wherever possible.

Be Wary of Scareware Tactics

Versions of software that claim to be free, cracked, or pirated can expose you to malware or social engineering attacks that attempt to trick you into thinking your computer is infected and getting you to pay money to have it removed.

Use an Effective Password Policy

Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or websites.

Use complex passwords (upper/lowercase and punctuation). Passphrases and password management apps can help too.

Think Before You Click

Never view, open, or copy email attachments to your desktop or execute any email attachment unless you expect it and trust the sender. Even when receiving email attachments from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails or social media communications, even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using a preview tool or plugin.
- Use a web browser plugin or URL reputation site that shows the reputation and safety rating of websites before visiting.
- Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop up asking you to install media players, document viewers, and security updates. Only download software directly from the vendor's website.
- Be aware of files you make available for sharing on public sites, including gaming, BitTorrent, and any other peer-to-peer (P2P) exchanges. Keep Dropbox, Evernote, and other usages to a minimum for pertinent information only, and only use when approved for corporate use.

Safeguard Your Personal Data

Limit the amount of personal information you make publicly available on the Internet (in particular via social networks). This includes personal and financial information, such as bank logins or birth dates. Additionally:

- Regularly review your bank, credit card, and credit information frequently for irregular activity.
- Avoid banking or shopping online from public computers (such as libraries, Internet cafes, and similar establishments) or from unencrypted.

Wi-Fi Connections

When using public wireless hotspots consider the following:

- Use HTTPS when connecting via Wi-Fi networks to your email, social media, and sharing websites. Check the settings and preferences of the applications and websites you are using.
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it
- Look for the green browser address bar, HTTPS, and recognizable trust marks when you visit websites where you log in or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.