CARICHAM
Centre of Excellence

arise
PRIVATE SECTOR ALLIANCE FOR DISASTER RESILIENT SOCIETIES

DIGITAL TRANSFORMATION

10 Tips to Protect Yourself Online

Ten Tips to Protect You Online

In both your professional and personal context, the use of digital tools continues to grow. Smartphones, computers, and tablet computers are all increasingly connected to our lives and the Internet. This provides an increasing opportunity for cybercriminals to carry out attacks targeted at an unsuspecting public.

The question is, how can you best protect yourself and others against these risks?

Here are ten things you can do to increase your digital security:

1. Protect your passwords

Use passwords that are long and complex. Most unauthorised access to information systems is from the use of easy-to-guess passwords. Dashlane, a password security company lists the top ten most common passwords in use in the US as:

1. Password
2. 123456
3. 123456789
4. 12345678
5. 1234567
6. Password1
7. 12345
8. 1234567890
9. 1234
10. Qwerty123

Use one password per account. This ensures that if one account is compromised, it won't automatically affect all your accounts. If you have the same password for all your different social media accounts, hackers can access them by compromising only one.

By using a password manager (see tools below) you can easily manage all your passwords in substantially increase the security of your information systems.

Ten Tips to Protect You Online

2. Backup your data regularly

The previous section talks about why and how you can securely backup your company's information. Backing up your data increases your security and increases your resilience in the case of disaster. Make sure you implement a robust backup strategy by following the guidelines and using the templates provided in the previous section.

3. Regularly apply updates to your applications

If you have applications running locally on information systems, PCs, mobile phones, and laptop computers, ensure that they are regularly updated.

Updates fix security bugs and add new tools to prevent malware and back door access.

BOX 1: Malware/Back Door

Malware: Malware is short for Malicious Software and refers to any software that is designed to steal data or damage/destroy computers and computer systems. Examples are viruses, worms, trojan horses, spyware, adware and ransomware.

Back Doors: Backdoors are undocumented and unauthorised ways of gaining access to computer systems.

Photo by Shahadat Rahman on Unsplash

CARICHAM Centre of Excellence

arise

Ten Tips to Protect You Online

4. Use antivirus/anti-malware systems

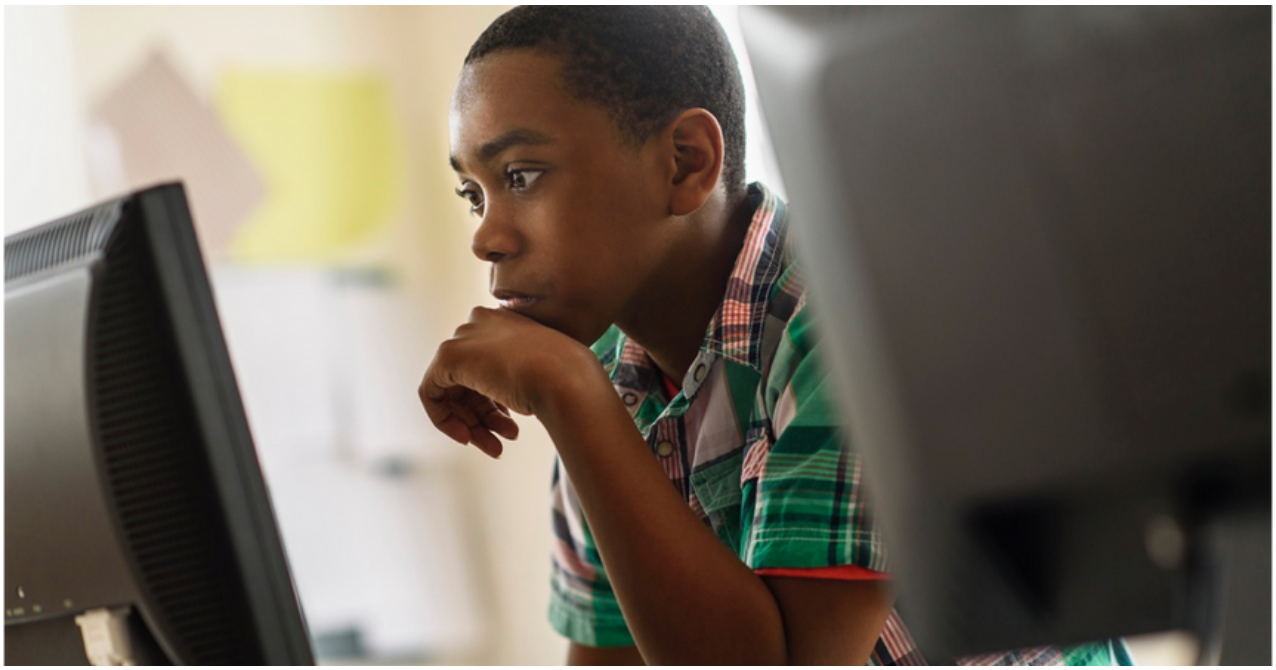
Antivirus and anti-malware systems that are regularly updated prevent a large number of security incidents and capture the majority of viruses and malware in the wild. There are many producers of these systems, including freeware to paid-for products and services. Choosing a reputable product is preferred and will save you a lot of time in the long run.

5. Only download software from official sources

Never download and install software from unknown sources or directly from emailed links or links sent through social media. On the Apple ecosystem (iPhone/iPad) you can only install software from Apple's App Store. On the Mac, you can install software from anywhere (by modifying a system setting), but installing software from Apple's Mac App Store is recommended.

On Android, you can install software from anywhere, but using the Google Play Store is recommended.

On Microsoft's Windows platform, Microsoft has its own store where you can download and install most of the applications you need.



CARICHAM Centre of Excellence

arise

Ten Tips to Protect You Online

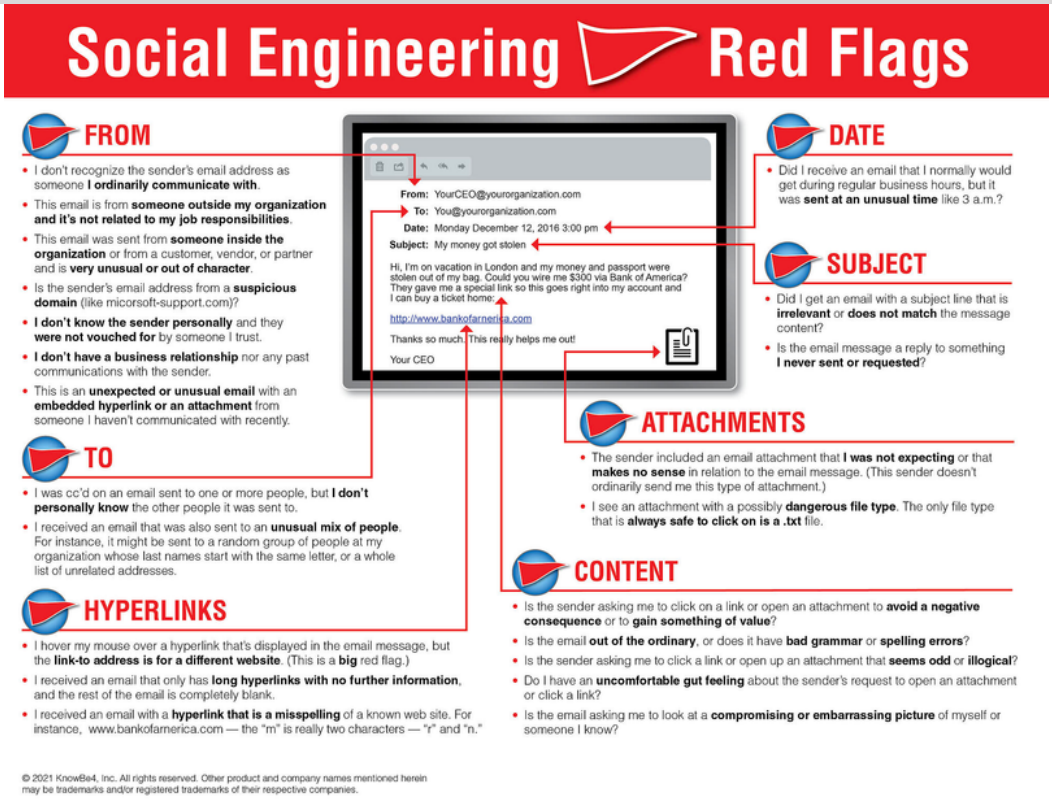
6. Be sceptical of any unwarranted messages

If you receive messages through email or social media from contacts that you either don't know or don't typically exchange with, be on alert that this could be a phishing or fraudulent attempt to gain your confidence. Generally, the one principle to use is:

If it looks too good to be true, it probably is!

BOX 2: Phishing (see image below)

Phishing is a type of social engineering that falsely claims to be from a legitimate person or organisation. It is typically used in scams to extract money through fraudulent schemes that involve banking, parcel deliveries, etc. (https://www.phishing.org/what-is-phishing)



Source: KnowBe4

CARICHAM Centre of Excellence

arise

Ten Tips to Protect You Online

7. Verify the legitimacy of websites you use to purchase goods and services

eCommerce has simplified the way we all buy products and has allowed us to benefit from special offers that we wouldn't otherwise have had access to, particularly here in the Caribbean. Sadly, there are many unscrupulous websites whose sole purpose is to fraudulently offer products that will never be shipped, or have had "issues" during the shipping process and prevent you from being refunded.

Ascertain the credibility of the merchant site by looking at independent reviews. You can additionally look at company registration documents in the country of origin (Companies House, Dunn & Bradstreet, etc) to see if it is a real company.

Remember: If in doubt, don't buy!

Ten Tips to Protect You Online

8. Manage your social networks

As tools for building and maintaining relationships both personal and professional, social networks offer incredible value for money. However, if used uncontrollably, they can lead to the leaking of personal details that can be used against you in a phishing attempt, for example.

Sophisticated and automated tools can now piece together a detailed picture of an individual by their photos, dates, places, and friends posted on social media sites like Instagram and TikTok.

Keep your personal and private conversations private by securing your accounts to keep public posting to a minimum. If you have to use social media in a public manner to build your brand or your notoriety, use a separate social media account specifically and only for this purpose.

9. Separate online personal and professional use

Be careful to separate personal and professional use of computer systems as much as is feasible. The ideal situation would be to have personal computer systems and accounts and professional systems and accounts. That is not realistically possible for most people. However, using a separate login to a personal computer can separate work and home use using two different accounts.

Some companies strictly forbid using professional tools for personal use, but this is not always the case. As the rise in Work from Home and Bring Your Own Device have shown, the lines between the two uses are becoming evermore blurred.

Just remember that if you use one account for all your needs, only one breach of this account can give access to everything in one fell swoop. With multiple accounts, systems, and logins, this is not possible **(see Tip Number 1)**

CARICHAM Centre of Excellence

arise

Ten Tips to Protect You Online

10. Avoid using unknown public wifi hotspots

When roaming (locally or abroad), stick to using known wifi systems from either people and companies that you know, known telecommunications companies (like Digicel and Flow) and/or local authorities - many public spaces are starting to provide free wifi to citizens through programs like those found in Trinidad and Tobago and in Jamaica.

Avoid using unknown public wifi hotspots!

If you have to use a public wifi system that you are unsure about, you can do so by installing and using a VPN, Virtual Private Network.

There are several simple-to-use VPN systems available. They provide security and privacy when using public internet. Remember to download them from trusted sources - See Tip No.5

BOX 3: Other resources

https://www.getsafeonline.org/get-safe-online-around-the-world/

Get Safe Online is the UK's leading internet safety website. We provide unbiased, factual and easy-to-understand information on online safety. Our website is a unique resource providing practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online. It contains guidance on many other related subjects too – including performing backups and how to avoid theft or loss of your computer, smartphone or tablet. Every conceivable topic is included on the site – including safe online shopping, gaming and dating … so you really can stay safe with everything you do online.