



&



TIPS FOR KEEPING YOUR DATA SAFE ONLINE

Create Complex Passwords



Downloading a password manager will create and store encrypted passwords and protect your accounts by keeping your passwords in a secure location. Make a habit of also regularly changing your passwords.

Protect Personal Information



Never give out personal information over the phone or through text. Most agencies, organizations, and companies would never ask for such information in this manner.

Beware of Links



Be cautious before clicking on links! Hover over any hyperlinks you receive in email or on web pages to preview their locations. Hackers disguise hyperlinks to look legitimate so people are enticed to click on them.

Two-Factor Authentication



Always enable two-factor authentication on your accounts. It might be tedious, but this is an extra layer of security designed to ensure that you're the only person who can access your accounts, even if someone knows your passwords.

Update Regularly



Update your phone, app, and browser software as often as you can. These updates often include new security updates that your current software may not have.





&



TIPS FOR KEEPING YOUR DATA SAFE ONLINE

continued from page 1

Secure Accounts



Set up the security configurations of your social network accounts. For example, in Facebook, you can prohibit third-party companies to collect your data.

Maintain Privacy



Publish minimal personal information to social networks. Do not click on advertising links and do not take entertainment tests. Consider using a VPN (Virtual Private Network) for browsing the internet to maintain anonymity online.

Ensure Encryption



Make sure that the web pages you visit are “HTTPS” encrypted. If the URL starts with only HTTP without the S, do not log in, and never enter sensitive data to the page.

Watch out for Wifi



Avoid using public Wifi hotspots, since most often, data is being collected through them. For example, shopping online in an airport using public wifi could potentially put your credit card information at risk.

Antivirus Protection



Antivirus protection software fends off computer viruses and ransomware that could encrypt your files and demand payment to restore them. You need antivirus to avoid Trojan horse programs that seem valid, but steal your private information.