accenture

STEPS TO STAY SECURE AT HOME OR ON-THE-GO

Secure Personal Devices

1. Make sure all your devices and Internet of Things (IoT) have the latest operating systems and software updates. Additionally, ensure your router firmware is current.
2. **Encrypt your devices** and set strong passwords or passcodes to prevent unauthorized access.
3. Use antivirus software—such as **Windows Defender** or **Malwarebytes**—and set it to update automatically to defend against the latest threats.
4. Only buy IoT devices from trusted manufacturers and disable any features you do not use. Don't place devices with cameras in rooms you wouldn't feel comfortable being seen by strangers.

Protect your Data while Traveling

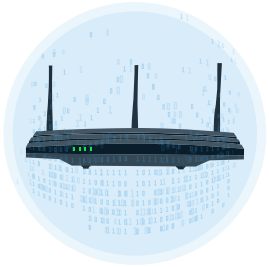
1. Never leave your devices unattended. If you need to step away, take everything with you or secure your laptop with a lock. Never rely on someone else to guard your belongings.
2. Use your own personal hotspot to connect to the internet. If you must use an unencrypted public network, confirm that the network is genuine prior to connecting and use the "Public network" firewall setting.
3. If you work in public spaces often, use a screen protector to shield sensitive information from prying eyes.

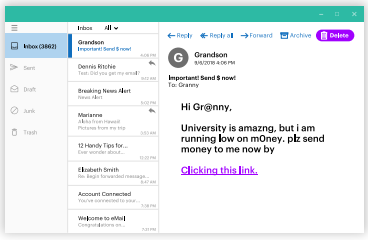
Protect your Accounts with Strong Passwords

1. Use a combination of capitals, characters, and numbers to strengthen your password.
2. Use multi-factor authentication (MFA) wherever possible. Facebook, Gmail, and most banks have multi-factor authentication available (click **here** for a list of sites with MFA available).
3. Use a different password for every account that you and your family hold. Leverage a password manager, such as **LastPass**, **dashlane**, or **1Password**, to make this easier.
4. Change the default credentials for your smart home or "Internet of Things" (IoT) devices.

Secure your Home Network

1. Make sure that you have done the following to secure your router.
   - Set the WIFI signal security to use WPA2 encryption.
   - Update your router with the latest firmware.
   - Change the admin password for your router settings page from the factory default. **Change your wireless network name and password** from the factory default setting.
2. For additional protection, filter internet access with **OpenDNS**. Change the DNS servers on your router to use the OpenDNS IPv4 addresses.





Don't Fall for Phishing

1. If you receive a suspicious email, do not click on links or download attachments. Always verify the authenticity of emails from unfamiliar senders with another form of communication. Beware of urgent requests for sensitive information as well as spelling and grammar mistakes.
2. If you see an ad offering something that sounds too good to be true, it probably is. Review the destination URL of any hyperlinks by hovering over them first. If the URL does not look familiar, don't click on it.
3. Before entering in any personal information like credit card numbers or login credentials into a website, make sure the URL in the address bar starts with https://, not just http://.