NATIONAL CYBER SECURITY AWARENESS

Protect Your Data
Be sure to encrypt sensitive data by using a program to protect your files.

Many systems offer this as an add-on feature of a security package. Two-factor authentication adds a second step to verify your identity.

Phishing Scams
Be aware that the most common cyber scams, cyber criminals can spoof email addresses to trick you into providing personal information. Do not click on any links or open any attachments or pop-up screens from sources you are not familiar with.

Keep Personal Information Secure
Hackers can use social media profiles to figure out your passwords and answer those security questions in a password reset tool. You can control how much information you share but not with all the hackers.

Keep Personal Information Personal
Lock your privacy settings as much as you can and watch the way things like birthdays, addresses, mother’s maiden names, etc. can be used.

Shop Safely
Before shopping online, make sure the website uses a secure protocol, look for the locked padlock symbol on the browser. Always check the URL to make sure the site is legitimate.

Prevent Isn’t Always Perfect
It’s true, albeit you are very judicious and legiti...mately look for the locked padlock symbol on the browser. Always check the URL to make sure the site is legitimate.

Phone Number Change or Loss
Tell your financial institutions immediately if you change your number or lose your mobile phone.

Avoid storing sensitive information like passwords or your security number on your mobile device.

Mobile Phishing
Avoid by changing the links in an email and avoid storing sensitive information on your device.

Regarding of an Old Device
Always be sure to update your operating system (whether or not it’s being manufactured anymore).

Enable Remote Wipe Feature
Remote wipe is a security feature that allows you or the network administrator to send a command to a computing device and delete data.

Online Banking
Always be sure to log off completely when you finish an online or mobile banking session.

Update Your Browser
Security patches are released for popular browsers all the time. You should always update your operating system or mobile phone to ensure that the latest security patches are installed.

For Firewalls
Firewalls can drastically reduce the risk of hackers and phishers infiltrating your computer or your network.

Use Antivirus
The software is continuously upgraded due to the new scams and threats.

Lock Your Computer
If your computer is infested with malware or viruses, your system administrator has the ability to send a command to a computing device and delete data.

Small Language
If you recognize the name in an email but the language doesn’t sound like them you should call to verify with the company.

Use System Update
Always make sure your software is updated and running. Mobile software is updated more frequently than desktop software.

Lock Your Computer
If your computer is infected.

Protective Password Practices
Create passwords and answer those security questions in a password reset tool. You can control how much information you share but not with all the hackers.

Unique Accounts, Unique Password
Having separate passwords for every account helps to better protect your accounts.

Complex passwords - that include combinations of letters, numbers & symbols - can better protect your accounts.

Secure Wi-Fi
Your computer holds a lot of sensitive personal information so be sure to lock it when you are not using it.

Lock the Computer
If you’ve left your computer unattended, be sure you are sure when they are supposed to be happening online or on your device.

Update Your Browser
Security patches are released for popular browsers all the time. You should always update your operating system or mobile phone to ensure that the latest security patches are installed.

Use Antivirus
The software is continuously upgraded due to the new scams and threats.

Lock Your Computer
If your computer is infected.

Protective Password Practices
Create passwords and answer those security questions in a password reset tool. You can control how much information you share but not with all the hackers.

Unique Accounts, Unique Password
Having separate passwords for every account helps to better protect your accounts.

Secure Wi-Fi
Your computer holds a lot of sensitive personal information so be sure to lock it when you are not using it.

Lock the Computer
If you’ve left your computer unattended, be sure you are sure when they are supposed to be happening online or on your device.

Small Language
If you recognize the name in an email but the language doesn’t sound like them you should call to verify with the company.

Use System Update
Always make sure your software is updated and running. Mobile software is updated more frequently than desktop software.

Protective Password Practices
Create passwords and answer those security questions in a password reset tool. You can control how much information you share but not with all the hackers.

Online Banking
Always be sure to log off completely when you finish an online or mobile banking session.

Download Mobile Apps
Use caution when downloading apps that they contain no obvious software errors, are obvious, reviews of apps that ask for unnecessary ‘permissions’.

Enable Remote Wipe Feature
Remote wipe is a security feature that allows you or the network administrator to send a command to a computing device and delete data.

Mobile Phishing
Avoid by changing the links in an email and avoid storing sensitive information on your device.

Getting Rid of an Old Device
Always be sure to update your operating system (whether or not it’s being manufactured anymore).

Prevent Isn’t Always Perfect
It’s true, albeit you are very judicious and legiti...mately look for the locked padlock symbol on the browser. Always check the URL to make sure the site is legitimate.

Phone Number Change or Loss
Tell your financial institutions immediately if you change your number or lose your mobile phone.

Avoid storing sensitive information like passwords or your mobile number on your mobile device.

Download Mobile Apps
Use caution when downloading apps that they contain no obvious software errors, are obvious, reviews of apps that ask for unnecessary ‘permissions’.

Enable Remote Wipe Feature
Remote wipe is a security feature that allows you or the network administrator to send a command to a computing device and delete data.

Mobile Phishing
Avoid by changing the links in an email and avoid storing sensitive information on your device.

Online Banking
Always be sure to log off completely when you finish an online or mobile banking session.

Update Your Browser
Security patches are released for popular browsers all the time. You should always update your operating system or mobile phone to ensure that the latest security patches are installed.

For Firewalls
Firewalls can drastically reduce the risk of hackers and phishers infiltrating your computer or your network.

Use Antivirus
The software is continuously upgraded due to the new scams and threats.

Lock Your Computer
If your computer is infected.

Protective Password Practices
Create passwords and answer those security questions in a password reset tool. You can control how much information you share but not with all the hackers.

Unique Accounts, Unique Password
Having separate passwords for every account helps to better protect your accounts.

Secure Wi-Fi
Your computer holds a lot of sensitive personal information so be sure to lock it when you are not using it.

Lock the Computer
If you’ve left your computer unattended, be sure you are sure when they are supposed to be happening online or on your device.

Small Language
If you recognize the name in an email but the language doesn’t sound like them you should call to verify with the company.

Use System Update
Always make sure your software is updated and running. Mobile software is updated more frequently than desktop software.

Protective Password Practices
Create passwords and answer those security questions in a password reset tool. You can control how much information you share but not with all the hackers.

Unique Accounts, Unique Password
Having separate passwords for every account helps to better protect your accounts.