NATIONAL CYBER SECURITY AWARENESS

tip 1

Protect Your Data

Be sure to encrypt sensitive data by using a program to password protect your files.

Stay Two Steps Ahead

tip 2

Many systems offer this as an added layer of security. Two factor authentication adds a second step to verify your identity.

tip 3

Phishing Scams

Phishing is one of the most common cyber scams. Cyber criminals use spoofed emails or fake websites to trick users into voluntarily disclosing personal or account information. DO NOT click on links or open any attachments or pop-up screens from sources you are not familiar with.

Keep Personal Information Personal

tip 4

Hackers can use social media profiles to figure out your passwords and answer those security questions in password reset tools. You can control how much information you share with the public

tip 5

Keep Personal Information Personal

Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc.

Don't Connect With Strangers

tip 6

Be wary of social media requests from people you do not know.

tip 7

Secure Wifi

Always be on a secure wireless network. Your home wifi should always have a password to access it and when you're using public wifi on the go be cautious about the information you're sending over it.

Shop Safely

tip 8

Before shopping online, make sure the website uses secure technology. At the checkout screen be sure to verify the web address begins with https. You should also look to be sure a tiny padlock symbol appears on the page.

tip 9

Pretty Isn't Always Perfect

Do not assume a company is legitimate based on the look of their website. Always check the URL to make sure the site is legitimate.

Email Cautious

tip 10

Don't click on links or open attachments in emails unless you can verify the sender or legitimacy of the email.

tip 11

Phone Number Change or Loss

Tell your financial institution immediately if you change your number or lose your mobile phone.

Mobile Phishing

tip 12

Avoid opening links and attachments in emails and texts, especially from senders you don't know, also be wary of ads (not from your security provider) claiming your device is infected.

tip 13

Lock Your Phone

Make sure you use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen.

Getting Rid of an Old Device?

tip 14

Always be sure to wipe them clean before you donate, sell or trade it using specialized software or using the manufacturer's recommended technique.

tip 15

Enable Remote Wipe Feature

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

Online Banking

tip 16

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

tip 17

Downloading Mobile Apps

use caution when downloading apps they can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions".

Protect Your Identity

tip 18

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

tip 19

Think Before You Click

It's ok to click on links on trusted sites. However, hyperlinks are commonly used to lead unsuspecting Internet users to phishing websites. Hover over links that you are unsure of and be sure they lead where they are supposed to before clicking on them.

Update Your Browser

tip 20

Security patches are released for popular browsers all the time. You should absolutely update anytime there is one available these updates fix security loopholes that phishers and hackers inevitably discover and exploit.

tip 21

Firewalls

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

Use Antivirus

tip 22

Be sure to keep your antivirus software up to date. Software is continuously upgraded due to the new scams being created everyday.

tip 23

Firewalls

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

System Updates

tip 24

Always make sure all software on your computer and mobile device is up to date. Newer software can better protect against the latest threats.

tip 25

Lock Your Computer

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

Email Language

tip 26

If you recognize the name in an email but the language doesn't sound like them you should call to verify with the sender before taking an action or downloading any attachments.

tip 27

Protective Password Practices

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

Protective Password Practices

tip 28

Change passwords routinely and keeping them private are the easiest and most effective steps your employees can take to protect your data. If you suspect a breach, immediately change passwords

tip 29

Unique Accounts, Unique Password

Having separate passwords for every account helps to thwart cybercriminals.

Be Cyber Aware

tip 30

Stay current. Keep pace with the latest threats and new ways to stay safe online and encourage friends and family to be Cyber Aware.

ConnectOneBank

a better place to be