METROPOLITAN CAPITAL

A UNIVERSAL BANK

Cybersecurity Awareness

Part 1: Staying in Touch

The pandemic drastically changed how people stay in touch, and the virtual space has become increasingly important. Don't be fooled by cybercriminals pretending to be your friends and family; always check the actual sender before you click on anything.

While using the internet, keep your personal information personal by using strict privacy settings. This will help to protect you against identity theft. It is also important to protect your social media accounts by using strong passwords and multi-factor authentication (MFA).

Info-Tech Research Group Inc. is a global leader in providing IT research and advice. Info-Tech's products and services combine actionable insight and relevant advice with ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2021 Info-Tech Research Group Inc.

INFO~TECH RESEARCH GROUP

Check the actual sender of a message

Every email, text message, and social media message will tell you who it was sent by. A powerful way to stop yourself from falling for a scam is to be absolutely sure that the sender is somebody you know and trust.

A dangerous phishing email may:

1. Look like it's from someone you know or a legitimate organization.
2. Ask you to download files (which may contain viruses).
3. Ask you to log into your account by clicking a link, which will direct you to a fake webpage where they can ask for and steal your credentials.
4. Have a vague email signature.
5. Contain spelling and grammar errors.



Remember: Treat every message with caution.

Keep your personal information safe

While keeping in touch with friends and loved ones online, we must be careful about who can see our information. Learn what information is considered sensitive, and limit who has access to it.

You should:

1. Carefully manage your privacy settings on any online service you use.
2. Share information only with those who you know and trust.
3. Be careful when you add people you don't know in the real world.



Remember: Be careful who you share information with.

Use strong passwords and enable MFA

Setting privacy access rules is not enough if your password can be easily guessed. Protect your account by creating strong passwords. Simple passwords like “123456” and “password” are easy to guess and should never be used. Secure your accounts even more by enabling multi-factor authentication (MFA), if it is available.

To protect your social accounts:

1. To limit the dam age a hacker can do if they steal your password, do not use the same password for all your accounts.
2. If it is available, use MFA to add another level of security that will protect you if your password is stolen.



Remember: Use unique and strong passwords for all your accounts.

Part 2: Sharing Special Moments

Your special moments are meaningful; don't let cybercriminals take advantage of them. When sharing memories with friends and family, always double check the files actually come from someone you know to avoid getting malware on your machine. It is also good practice to back up your important files regularly, to prevent losses from cyberattacks or accidents.

Info-Tech Research Group Inc. is a global leader in providing IT research and advice. Info-Tech's products and services combine actionable insight and relevant advice with ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2021 Info-Tech Research Group Inc.

INFO~TECH RESEARCH GROUP

Staying safe while sharing files

Files that are shared with us are not always from your friends and family – they may be sent by a person with bad intentions. Always double check the file sender when you are invited to click a link or download anything onto your machine.

When you receive an attachment:

1. Watch out for email and text messages asking you to click on links or download files.
2. Read messages carefully – phishing messages often contain spelling mistakes.
3. Understand that files can appear to be safe, but when clicked on, could install malicious code onto your device.



Remember: Always double check the sender before clicking or downloading.

Be aware of potential malware

Links and files from unexpected emails may install malware on your machine when clicked on. This malware may steal your information, make your device unusable, ask for payment, etc.

To avoid being infected by malware:

1. Do not click on links or download files from senders you do not recognize.
2. Update your antivirus software and operating system as soon as updates are available.



Remember: Treat every link and downloadable file with caution.

Back up your data

Under the worst circumstances, malware can cause your files to become lost or corrupt. To help protect your important memories and special moments, back them up regularly.

It's best practice to:

1. Back up your data to help protect it against accidents, technology failure, and cyberattacks.
2. Consider using hard drive storage, cloud storage, or both when creating backups.
3. Update backups regularly to avoid losing new information.
4. Try not to back up information if you think your device is infected, as this could infect the backup.



Remember: Back up your data, and back up often.

Part 3: Working and Networking

Working at home poses new challenges to the workplace, as there are new cyberthreats to protect yourself against. It requires each person to take up the responsibility of creating a secure working environment at home.

Info-Tech Research Group Inc. is a global leader in providing IT research and advice. Info-Tech's products and services combine actionable insight and relevant advice with ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2021 Info-Tech Research Group Inc.

INFO~TECH RESEARCH GROUP

Connecting to the internet safely

Set up a secure working environment at home to help protect yourself and your work from harm. Be especially careful when connecting to the internet over Wi-Fi.

To create a safe environment:

1. Change Wi-Fi name and password from default settings.
2. Do not include personal information in Wi-Fi name or password.
3. Create a separate network for smart devices.
4. If available, use a virtual private network (VPN) at home.
5. Never use public Wi-Fi to access sensitive information.



Remember: Take the time to secure your working environment.

Workplace cybersecurity threats

Some cybercriminals will specifically target your organization account and send phishing emails to your work email. Be careful and always double check the sender.

Be careful:

1. Sometimes phishing scam s may pretend to be from a legitimate organization, your co-worker, a friend, or family member.
2. Before clicking on anything in an email, look for signs of a potential phishing attack, such as poor spelling or the email being unexpected or from an unknown sender.
3. Cybercriminals may try to socially engineer you in other ways, including over the phone or by text.



Remember: Treat messages, especially those that are unexpected, with caution.

Part 4: Families and Businesses

While staying vigilant about cyberthreats, you must also understand the threats posed to families and small businesses and how you can protect against them. Not everyone in your family is well informed on cyberthreats. Children are particularly vulnerable due to the lack of awareness they may have for staying safe online. For businesses, the shift to remote work creates new security challenges because employees likely have no prior experience in performing duties remotely. Employees must be taught how to work from homes securely.

Info-Tech Research Group Inc. is a global leader in providing IT research and advice. Info-Tech's products and services combine actionable insight and relevant advice with ready-to-use tools and templates that cover the full spectrum of IT concerns.
© 1997-2021 Info-Tech Research Group Inc.

INFO~TECH RESEARCH GROUP

Keeping children and families safe online

Everyone on the internet can be targeted for cybercrimes, including children and other members of your family who may not be as well prepared for these challenges. Help your family members stay safe by teaching them best practices and restricting downloading access with parental controls.

Some things you can do:

1. Teach children about what is safe to share online and how to protect their accounts.
2. Enable parental controls where possible.
3. Share knowledge learned from the workplace with your family.
4. Ensure all devices at home are running up-to-date antivirus program s to prevent infection.



Remember: Your family is vulnerable to cyberthreats as well.

Running a cybersafe business

For businesses where remote work may not have been required prior to the pandemic, training your employees on how to stay safe while working remotely becomes an important task.

Some things you can do:

1. Create strong security policies that include information pertaining to working from home.
2. Raise employee security awareness through training and activities.
3. Provide technology that can help users secure their remote working environment.
4. Encourage employees to share security knowledge with their families to better protect the home network.



Remember: Train your employees on how to safely work remotely.