Bharat National Public School/ HES

Cyber Security Awareness Month- October 2020

Do your Part

#BeCyberSmart

Steps to protect your Digital Home

More and more of our home devices—including thermostats, door locks, coffee machines, and smoke alarms—are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which in turn can save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing, however they also pose a new set of security risks. #BeCyberSmart to connect with confidence and protect your digital home.

SIMPLE TIPS

- **Secure your Wi-Fi Network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username. For more information about protecting your home network.
- **Double you login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Back up your data.** These days, storage doesn't cost much. There's no excuse not to have a backup of important data. Back it up on a physical location and on the cloud. Remember, malicious threats and hackers don't always want to steal your data, but sometimes the end-goal is to encrypt or erase it. Back it up to have an ultimate recovery tool.
- **You're Not IMMUNE.** The most harmful thought you can have is "it won't happen to me," or "I don't visit unsafe website". Cybercriminals don't discriminate in targeting all sorts of users. Be proactive. Not all mistakes can be undone with "ctrl+ Z". Simple cyber security tips like these can go a long way in preventing a catastrophe. But they've only scratched the surface of how users can be educated and protected.

Be Aware …… Be Secure

Bharat National Public School/ HES

Cyber Security Awareness Month- October 2020

Do your Part

#BeCyberSmart

Steps to secure on Social Media

Now more than ever, consumers spend increasing amounts of time on the Internet. With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world. How can you be proactive and “Do Your Part. #BeCyberSmart”? Take these simple steps to connect with confidence and safely navigate the social media world.

Did You Know?

- In 2020 3.81 billion people worldwide now use social media worldwide. That’s an increase of more than 9% from 2019. Put another way: 49% of the total world population are using social networks.
- Digital consumers spend nearly 2.5 hours on social networks and social messaging every day.

Simple Tips

- **If You Connect IT, Protect IT.** Whether it’s your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software. Read the Phishing Tip Sheet for more information.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don’t realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren’t—at any given time.
- **Speak up if you’re uncomfortable.** If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you’ve posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them, and it is important to respect those differences. Don’t hesitate to report any instance of cyberbullying you see.
- **Report suspicious or harassing activity.** Work with your social media platform to report and possibly block harassing users. Report an incident if you’ve been a victim of cybercrime. Local and national authorities are ready to help you.
- **Remember, there is no ‘Delete’ button on the Internet.** Share with care, because even if you delete a post or picture from your profile seconds after posting it, chances are someone still saw it.
- **Connect only with people you trust.** While some social networks might seem safer for connecting because of the limited personal information shared through them, keep your connections to people you know and trust.

Be Aware …… Be Secure