Tips to stay safe online and PROTECT YOUR PRIVACY

TASNUVA KINNORI

Digital security means safeguarding against cybercrime and other security risks while navigating the internet. With millions of people worldwide working, studying or socializing strictly online, our virtual lifestyles are more exposed to cyber threats than ever before.

According to the UN, cybercrime is up by 600% due to the Covid-19 pandemic. Such alarming statistics only emphasize the importance of taking certain precautions to bolster our digital safety:

Be careful where you click

The internet is filled with suspicious websites, emails, pop-ups, online quizzes and links that steal your private information or sneak in viruses and malware onto your device. Before clicking on a link claiming you won a crazy prize, try to spot the tell-tale signs of deceit, such as- click-bait headlines, poor grammar, pop-ups, or web addresses that seem phony. Visiting such sites, providing any sort of information on the site or downloading anything from there can result in your data being stolen, accounts being invaded or devices getting infected with viruses.

Keep your software updated

That annoying software update request that you keep putting off may contain important security updates for your device or OS. Staying up-to-date with the latest version of software patches up identified holes in your device's security- providing the best possible protection against constantly changing threats. To get the latest updates soon as they're released, simply enable automatic updates in your device's settings.

Stronger passwords, better security

While using a strong password may seem obvious, setting easy to guess passwords or the same one across multiple accounts is a common practice. There exist many general guidelines to set strong passwords, such as having both lower and upper case letters, using numbers or signs etc. If setting an easy to remember but hard to crack password is too much of an inconvenience, try utilizing a password management tool which generates complex passwords as well as stores them for you. There are many free password management tools available for use, such as LastPass, Avira Password Manager, RoboForm etc.

Layered security with multi-factor authentication

Multi-Factor Authentication increases the security of an account by asking for additional information, such as- codes delivered via SMS, security questions or biometrics to authorize logging in. This service is available for most email providers and social media platforms. To see if a website supports multi-step authentication, check the site's settings page. While the extra steps may seem inconvenient, your data will be much safer than with just a password.

Account management

Our increased online presence comes with an increase in the number of accounts we use across the internet. Managing all these accounts is a fundamental step in ensuring our digital security.

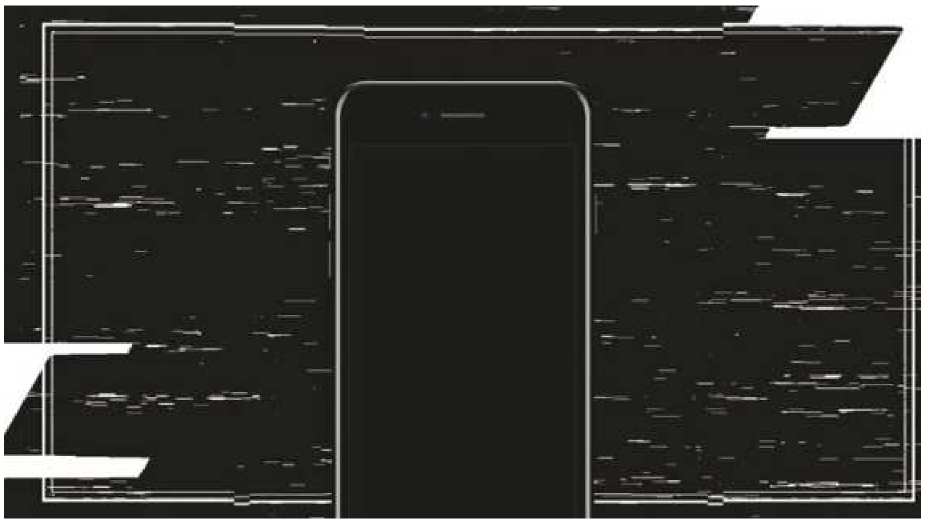

ILLUSTRATION: **ZARIF FAIAZ**

Firstly, any account that is no longer in use should be deleted. Secondly, it's best to log out of accounts after use- be it on social media, e-commerce platforms or sites holding sensitive information (like bank account or credit card info). Since logging into these websites creates cookies in your browser (which if stolen, can compromise your account), logging out is the safest. Logging out of personal accounts is also crucial while using public computers or networks.

For private devices, it's typically safe to stay logged on to email accounts or social media, as long as the device itself is securely locked with pins or passwords. For social media accounts, it's important to review profile visibility and privacy layers to prevent strangers from getting ahold of your personal information. Additionally, turning on tag reviews in the privacy settings can help in cases of being tagged in unwanted/ potentially harmful posts without your approval.

Ensure network security

Open networks, such as public Wi-Fi hotspots leave you with no direct control over the security of the connection. While it's best not to connect to such networks, if it is unavoidable, using a secure VPN (Virtual Private Network) is recommended. A VPN establishes a secure network connection between your device and an internet server, ensuring that no one can monitor or read the information exchanged. For sharing sensitive information like- addresses or bank details, make sure you're connected to a secured private network.

Antivirus and firewalls

Other than installing antivirus software for your computer, you can also use antivirus extensions on a mobile browser to check a site's security and prevent pop-up advertising that may contain viruses. Moreover, setting up firewalls is an effective way to prevent any unauthorized access to your computer or phone. While some devices come with pre-installed firewalls, for those that don't, most antivirus packages provide firewall protection too.

Secure your downloads

Downloads are the most common route for viruses to enter your devices. Apps obtained from official sources such as the Apple App Store or the Google Play Store are safer than downloading anything from third-party sites. Before installing anything, make sure to go through the permissions, terms and conditions- which will undoubtedly be a tedious process, but is critical to understand what you are inviting onto your devices.

Clear out history and cookies

Trying to scroll down on a website only to have the content blocked out by an annoying "This Website Uses Cookies" pop-up? These cookies are text files that record your preferences, allowing websites to (typically) show you more relevant advertisements. On the other hand, hackers can exploit these cookies to obtain your personal information. Thus, clearing your browser history and cookies every month or so ensures that any trackable personal information stored in them is removed.

Securing mobile devices

Smartphones are the most used devices to access the internet, making them a prime target for security breaches. Some general tips to boost your mobile security include- using biometrics, facial recognition or difficult passcodes to unlock the device, keeping the OS updated, performing regular mobile backups and using in-built device tracking services to prevent loss or theft. Smartphones now come with encryption software that scrambles data so unauthorized parties can't access it.

To see if your device is encrypted, check the security tab under the device's settings. If your device doesn't come encrypted out-of-the-box, encryption apps can be downloaded from verified sources for more security. For an extra layer of security, toggle Bluetooth settings to "non-discoverable" in crowded places.

Making online payments

The virtual payment for all your online shopping exploits may be a prime opportunity for hackers to obtain your banking information. To see if a payment gateway is secure, look no further than the website's address- which should begin with "https" (instead of only "http") and the URL field displaying a padlock icon. Also, keep an eye out for addresses with misspellings or poor grammar- which may be knockoffs of reputable sites. To avoid visiting dangerous websites, install safe search browser plug-ins.

Routinely review security settings

For all our online accounts, it's important to periodically change passwords and run security checks. As online security threats keep evolving, so should your digital security measures. While reviewing the security settings for any account, make sure to enable log-in notifications and change the security questions/ identity verification methods for multi-factor authentication.

For social media accounts, routinely review the privacy settings (especially after editing your profile), what information is available to the public and your personal information provided.

Backup data regularly

The recent trend in online threats sees a rise in "ransomware"- where hackers threaten to lock users out of their files unless a ransom is paid. The often-overlooked habit of backing up your devices' data to cloud storage or an external hard drive can provide a way around such online threats. Besides, even if your device gets infected by malware, regular backups will always save a copy of your valuable data.

Privacy Policies

For those looking to go the whole nine yards for their digital security, the largely ignored "privacy policy" accompanying apps, games, software and websites can explain how they secure and use the information collected from users.

AKM Fahim Mashroor, CEO, Bdjobs and Sumon Ahmed Sabir, CEO, Fibre at Home, were consulted in preparing this article. Find this article online on our website to read a detailed version with their quotes.