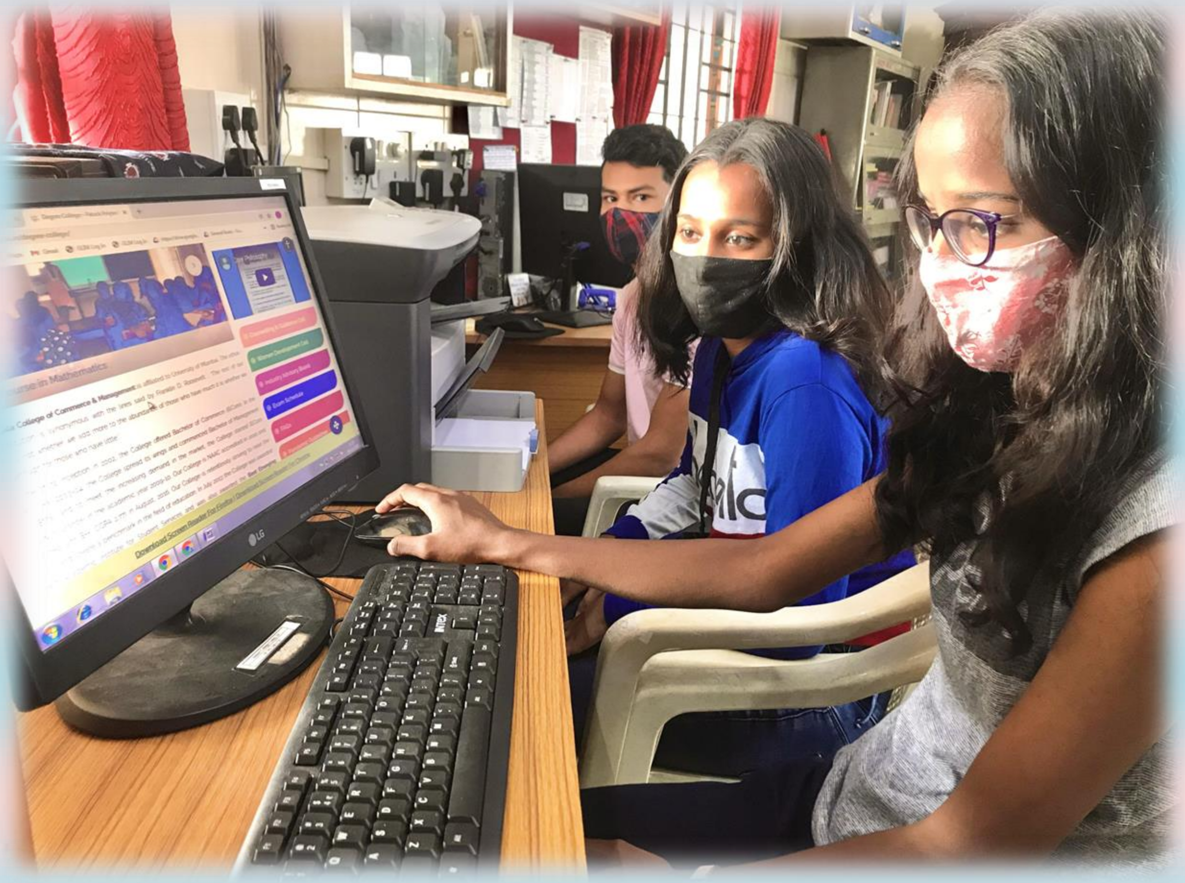
PATUCK-GALA COLLEGE OF COMMERCE & MANAGEMENT

STUDENT BULLETIN BOARD

NOVEMBER 2021

STAYING SAFE ONLINE



The Internet can be a wonderful place to network, learn, shop, play games, and connect with friends. However, careless internet habits can expose you to scams, identity theft and even physical harm due to the miscreants you meet online. These are the online predators, identity thieves, and people who may try to harm you. As youngsters, you may not always think about the consequences of your actions, which can result in you sharing too much information about yourself. With more people accessing the Internet through mobile devices, these risks are changing and growing quickly.

With more and more apps being used in almost all daily interactions, hackers are on the lookout for personal information they can use to access your credit card and bank information. Unsafe surfing can also lead to other threats—from embarrassing personal comments or images that, once online, are nearly impossible to erase, to getting mixed up with people you should be avoiding.

Here are the Top 10 Internet safety rules to follow to help you avoid getting into trouble online (and offline).

1. Keep Personal Information Professional and Limited

The public at large does not need to know your personal relationship status or your home address. Only the employers where you are applying for a job, may know about your expertise and professional background, and there will be professional emails for such interactions.. You should not hand purely personal information out to strangers individually—or put it out on social media which effectively means that you are handing it out to millions of people online.

2. Keep Your Privacy Settings On

Marketing companies, advertisers love to know all about you, and so do hackers. Through artificial intelligence and built-in applications, they can learn a lot from your browsing and social media usage. But the good news is that you can control your information. Both web browsers and mobile operating systems have settings available to protect your privacy online. Major websites like Facebook, Instagram also have privacy-enhancing settings available. These settings are sometimes (deliberately) hard to find because companies want your personal information for its marketing value. Make sure you have enabled these privacy safeguards, and keep them enabled.

3. Practice Safe Browsing

In real life, you would not choose to walk through a dangerous road. Similarly avoid visiting dangerous websites online. Attractive pop-ups, tempting pictures with clicking options might keep coming up on your screen while you browse your usual browsing. One careless click and you could expose personal data or infect your device with malware. By resisting the urge, you are not only saving your device from hacking but also your own safety and money. *All that glitters is not always gold.*

4. Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection

When you go online in a public place, for example by using a public Wi-Fi connection, where you have no direct control over its security. Make sure your device is secure, and when in doubt, wait for a better time (i.e., until you're able to connect to a secure Wi-Fi network, like in your college) before providing information such as your bank account number.

To further improve your Internet browsing safety, use secure VPN connection (virtual private network). VPN enables you to have a secure connection between your device and an Internet server that no one can monitor or access the data that you're exchanging.

5. Be Careful What You Download

A top goal of cybercriminals is to trick you into downloading malware—programs or apps that carry malware or try to steal information. This malware can be disguised as an app: anything from a popular game to something that checks traffic or the weather. Do NOT download apps that look suspicious or come from a site you don't know.

6. Choose Strong Passwords

Passwords are one of the biggest weak spots in the whole Internet security structure. Select strong passwords that are harder for cybercriminals to crack. A strong password is one that is unique and complex—at least 15 characters long, mixing letters, numbers and special characters. Make a habit of changing your password on a regular basis.

7. Make Online Purchases from Secure Sites

Any time you make a purchase online, you need to provide credit card or bank account information—just what cybercriminals are most eager to get their hands on. Only supply this information to sites that provide secure, encrypted connections. You can identify secure sites by looking for an address that starts with *https:* (the S stands for *secure*) rather than simply *http:* They may also be marked by a padlock icon next to the address bar.

8. Be Careful What You Post

The Internet does not have a delete key. Any comment or image you post online may stay online forever because removing the original (say, from Facebook) does not remove any copies that other people made. There is no way for you to "take back" a remark you wish you hadn't made, or get rid of that embarrassing selfie you took at a party. Don't put anything online that you would not want your family or a prospective employer to see.

9. Be Careful Who You Meet Online

People you meet online are not always who they claim to be. Worse, they may not even be real. Fake social media profiles are a popular way for hackers to catch unaware young Web users and exploit them. Be as cautious and sensible in your online social life as you are in your in-person social life.

10. Keep Your Antivirus Program Up to Date

Internet security software cannot protect against every threat, but it will detect and remove most malware—though you should make sure it's to date. Be sure to stay current with your operating system's updates and updates to applications you use. They provide a vital layer of security.

Keep these 10 basic Internet safety rules in mind and you'll avoid many of the nasty surprises that lurk online for the careless. Be smart. Be safe.

Sources:

1. https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online
2. https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
3. https://staysafeonline.org/stay-safe-online/
4. https://us.norton.com/internetsecurity-kids-safety-stop-stressing-10-internet-safety-rules-to-help-keep-your-family-safe-online.html
5. https://edu.gcfglobal.org/en/internetsafetyforkids/teaching-kids-about-internet-safety/1/

Cover picture features: Pratima Sonawane, Sanjana Singh & Akhilesh Vishwakarma