If you are part of Gen Y, connectivity is an important part of your daily life. But while tweeting, friending, and googling may be routine, are you protecting yourself online?

According to a recent Zone Alarm survey of 1245 participants, the majority of Gen Y* respondents leave Internet security on the back burner. Only 31% of Gen Y participants rank security as the most important consideration when making decisions about their computer. Gen Y was more likely to prioritize entertainment and community above security. However, half (50%) of all Gen Y indicated that they have had computer security issues in the past two years.

The research shows that Gen Y is leaving themselves — and anyone with whom they communicate — wide-open and vulnerable to online attacks. So, when you consider the growth of cybercrime in our over connected, always-on society, it doesn't hurt to be one-step ahead in the security game.

HERE ARE 10 WAYS TO KEEP OUT OF HARM'S WAY.

1. Get back to the basics. Regularly updating your computer's operating system is one of the simplest, yet most important, ways to protect your computer. The newest software versions help your system run more smoothly and prevent you from becoming vulnerable to holes found in your old system. Make sure your operating system is configured to receive automatic updates for the latest security patches, and be sure to apply the latest settings by restarting your computer after the updates occur.
2. Don't be click-happy. Did you know that 9500 malicious websites are detected by Google every single day? This stat includes legitimate sites that have been hijacked and those that are designed to spread malware. Stay safe by being wary of the links you click. And remember to hover over links so that you can review the full address before you click. You should also take the warning messages from Google to heart. And, always keep your firewall and antivirus up-to-date and active.
3. Pay attention to the latest social changes. For example, Facebook recently changed your default email to @facebook.com. This means that a whole new group of marketers and spammers will be able to contact you much more easily than ever before. Whether you Like this (or not), adjust your privacy protection settings and watch out for spam and phishing scams now that Facebook's messaging system is open.
4. Passwords, passwords, passwords. Always create strong passwords for all online accounts, and include letters, numbers, and symbols. Longer passwords are more secure and harder to crack. Choose different and unique passwords

for important sites, such as your primary email and financial accounts. Try not to use the same password for multiple sites. If a password gets compromised on one site, it may allow hackers to log into other accounts with the same credentials.

5. Gamers, keep your security software on deck. If you are serious about online gaming, don't disable your security software to play thrilling titles, like Diablo III. Yes, experiencing a high speed connection with minimal interruptions is important – but not at the expense of security. Instead, look for "Game Mode" in your security software. This setting will never interrupt you while you're in the middle of your game. At the same time, it will keep you protected.
6. Protect yourself against P2P and pirated software. The best solution is to simply never use P2P sites to download pirated software and, instead, download your files from the original software developer. But if you still choose to take that risk, you should at least take a few precautions, like reading the user comments before you download the file. Keep in mind that many of today's popular P2P sites offer a pretty accurate rating system that can provide you with a sense of just how these downloadable files have performed for other users.
7. Beware of social engineering attacks. Cybercriminals are scouring social media sites every day to learn all they can about you. They'll use the information they gather to send you highly targeted emails, pretending to be from your boss, friend, or family member. Did you post some information on Facebook recently about your favorite vacation spot – only to receive an email from a co-worker about the best summer getaways, complete with a request to link to a recent article? Stay on guard. And always watch what you say online – revealing too much information like middle names, pet names, etc. could be just enough to tip off a cybercriminal.
8. Choose your friends carefully. There's nothing like making connections online via Facebook and other social networks. However, you definitely put yourself at risk by not taking the time to filter who you accept into your inner circle. If you get a friend request from someone you haven't spoken to in years or someone you don't know, a social bot may be using this as an opportunity to hack into your network. They could exploit the trust you have built on Facebook and Twitter to send emails or notifications to your networks – using your access, information and persona to solicit products and spread malware to others' computers.
9. Take Care When Downloading Videos. Online video has really taken off– especially for Gen Y who often spends more time watching videos online than any other group. Be careful when downloading videos – as this activity could be a hotbed for viruses. If you don't have the most up-to-date video player,

download it directly from a trustworthy source. Never install software from file-sharing sites when trying to view a video, and keep in mind downloading a video by itself should never require running an executable (.exe) file.

10. Be Cautious When Using Wi-Fi Hotspots – Most people are thrilled when they encounter free Wi-Fi hotspots. But before you connect, verify that the Wi-Fi network name (SSID) is from a legitimate service. Do not connect to random, unsecured Wi-Fi networks. It increases your security risks. And use a Virtual Private Network, if you can. A VPN allows you to route all your activity through a separate, secure, private network, even if you're on a public one. Several services are available, or you can even go with an app like Hotspot Shield, which sets a VPN up for you automatically.

Staying vigilant is a good start. But it's just not enough. Cybercriminals are becoming craftier by the day, and online attacks are never ending. Whatever you do, it's important to take basic precautions by following the tips above and making sure you at least have antivirus software and a 2-way firewall on your computer. Don't be lulled into a false sense of security – no matter what your age. You will not only avoid becoming another statistic, you'll also do your part to keep the Internet safe for your online community