5 Cybernetic Threats to Push You off the Cliff

Mahidul Alam
Technical Consultant, Researcher, NRD Bangladesh Limited

Technological innovations improve communication and enable business expansion. At the same time, they are charged with increasingly well-planned scams, via fake news and bots, or easy-to-use cyber threats, but still capable of capturing hundreds of victims. Cyber threats act in bad faith on inattentive users to achieve greater Internet goals.

The attackers target innocent victims, usually children and the elderly, who easily click on traps, download malicious files, buy non-existent products or insert personal data in dubious forms.

From my observation, in fivemost smart ways the attacker can victimize you.

1 LOSE 10 KG IN 2 MONTHS

Techniques such as "how to lose weight fast", "how to lose weight without effort" or "learn the formula that made the actress plunge the belly" are hype marketing. These calls take a ride with the dangerous tendency of overestimation of the body allied to the underestimation of physical exercise. Everything that is sold as too easy, too fast, with immediate results and "no need to leave home," distrust.

Incredible promotions, magic coupons, eye-popping discounts and unique gifts are also part of the attraction. Watch out for site signs and fake contacts (secure browsing is certified by https - HyperText Transfer Protocol Secure, which must precede the e-mail address). Before clicking, do a quick search on the Internet about the brand and reputation of the products in question.

(And just consider weight-loss methods with a nutritionist or physical educator).

2 YOUR COMPUTER MUST BE FORMATTED

If your computer has crashed, is slow, or does not turn on, calm down! Do not go out looking for any technical repair service out there. Try less via chat. Find trusted professionals, contact a friend who has computer skills, and try to understand the problem before seeking help.

Online scammers phone the victim and try to convince his/her that there is a very serious problem with the computer. Sometimes they ask the user to format, send sensitive data or to transfer files. And they always impose an advance amount to pay for the work that will be "remotely solved."

In this "remote solution," the scammer can access the victim's information and even install malicious software - without her noticing.

The problem is not in the format button, but in the consequences after this action.

3 YOUR CARD WAS CLONED

Also known as phishing, or "fishing," identity theft is a classic that still fools a lot of people. The fake website or e-mail usually uses a visual identity that is close to reality. "Everything is designed to really confuse the user." It is common to send messages using known brands and logos from government agencies, credit card companies and banks, and even from well-known NGOs improperly.

According to experts, the main topics in phishing emails are invitations to social networks, emails with errors or failed to deliver, and "important communications."

When dealing with messages that express some emergency action, stay tuned. If your card has been cloned, for example, you will hardly have to make serious and urgent decisions on online platforms.

If in doubt, call the company's official contact.

4 DO YOU WANT TO MAKE MONEY?

CLICK HERE Spams also have their place.

These types of emails fill your inbox and offer everything from free cloud hosting services to baldness remedies.

Do not fall for obvious answers like "Do you want to make money?" Be careful where you click, and see if the question really does have a relevant answer.

Think: Making money is a universal goal without magic and sure formula. There would be no better trigger than this to win hundreds of innocent clicks.

5 YOUR COMPUTER HAS BEEN INFECTED. LOWER OUR ANTIVIRUS

Scareware is software that tries to trick the user into taking a certain download action. Generally, a vibrant colour alert flashes on the screen telling you that your computer has been infected and that you need to urgently install certain antivirus to protect yourself.

When this happens, close all tabs, all windows. Restart your computer and download absolutely nothing.

Never stop buying or installing a good antivirus so you can always have a place to go in these situations. Choose famous and reputable brands for antivirus software. Perform regular analysis and cleaning throughout your computer's internal system.

Never risk installing anti-virus that nobody has ever heard of.

It goes without saying that, we the end user have to be more cautious while using internet and must need to feel the words - the virtual world over internet you see, that cannot be touched. But it can harm an incautious user such a way which can be no less than a physical injury.

Hope this article will make you think about using internet with proper awareness, and here my intention for writing this article will fulfil