- Computer crimes

How to spot the top five most common cyber attacks

In recent years, cybercriminals have become more sophisticated in their attempts to mount threats against organizations, such as banks. But most of the time, cybercriminals are more focused on individual consumers as they are the more gullible and vulnerable targets in any cybercrime game, considering that they do not have defense systems as formidable as those in structured organizations.

Making the situation worse, many consumers have developed a carefree and complacent attitude toward these threats, in spite of the increasing reports of fraud surfacing in the news. Or perhaps, consumers have this kind of behavior simply because they are not aware of the cyber threats surrounding them.

Apart from investing heavily in technology to strengthen its cybersecurity system, the Bank of the Philippine Islands (BPI), the oldest bank in the country still in operation, is also relentlessly investing in educating its consumers regarding the existing cyber threats targeted toward them.

"When it comes to scams like hacking, phishing, and baiting, most of us see ourselves as the last person to fall victim to such scams. But this is exactly the kind of thinking that social engineers bank on," says Jonathan John B. Paz, BPI Enterprise Information Security Officer and Data Privacy Officer.

Social engineering is defined as the act of deceiving people into divulging their private information, by means of exploiting particular qualities of human decision-making known as cognitive biases. While hackers focus on attacking computers and online systems to steal information, social engineers put emphasis on manipulating people into allowing legitimate access to confidential information.

"And although social engineers mostly use technology to carry out their attacks, their deception has spread online and offline. Our best defense against these attacks, therefore, is to educate ourselves so that we recognize them as they happen," Paz added.

JONATHAN JOHN B. PAZ
BPI Enterprise Information Security Officer and Data Privacy Officer

Here are the five most common cyber threats directed toward consumers, how to spot them, and avoid being a victim:

1. Baiting – This technique banks on the natural curiosity of people. For example, an attacker leaves a malware-infected device like a USB flash drive in a public area such as a bathroom or a cafeteria. The attacker assumes that someone who finds the device will use it on a computer, unknowingly installing the malicious software.

2. Pretexting – This technique might require physical contact between the social engineer and the victim. For example, the attacker may pretend that he or she is part of the company's IT department to acquire an individual's or organization's passwords and other confidential information.

3. Phishing – The most common social engineering scheme, phishing happens when an attacker sends an email, IM, comment, or SMS that appears coming from a legitimate or popular company, bank, school, or any other institution. Recipients are misled into sharing confidential and valuable information, such as credit card or bank account numbers and PINs. Typically, the content of a phishing message informs recipients that there is a problem on their account and they are encouraged to verify information by clicking a link and putting details on an online form.

4. Spear phishing – As what its moniker suggests, spear phishing is a highly targeted type of phishing attack. Social engineers employ personal information derived from the target's social media account in order to gain that person's trust and appear legitimate. The more specific the phishing attack, the higher chances of success for the cybercriminal.

5. Tailgating – Another social engineering tactic that might require physical contact, one example is when an unauthorized individual follows an authorized person into a secure location. The attacker ensures that the victim will be in a situation wherein he or she must lend a device like a laptop or a smartphone. Pretending to be in an urgent need to email or search something online, the attacker actually installs malware or steals information from the device.

"In this day and age, it's safe to assume that all sources are suspicious. No matter how legitimate an email appears, it's safer to type a URL into your browser instead of clicking on a link. Don't open attachments from suspicious sources. These are things most of us already know, but often overlook," Paz warned.

"Social engineers count on their targets to follow routine and act mindlessly. Pause and ask whether that email from the bank is legitimate, if that message from "IT" has any basis, or if that humanitarian cause has set up alternative channels for donations. And as the adage goes, it's better to be safe than sorry," he added.