THE HINDU Business Line

Don't be a victim of cyber crime

K.V. KURMANATH

January 23, 2012:

Searching online for a good bargain to snatch an iPhone or a Samsung Galaxy S2? A good number of Internet users regularly visit online retailers to find out prices, features and discounts. Surveys have shown that e-commerce in India has picked up even in rural areas. Convenience, ease and great deals on offer have resulted in a spurt in online shopping. This is good news for retailers.

Unfortunately, it's good news for hackers too. As online shopping becomes the most preferred method for purchasing items, online shoppers will also become the most preferred cybercriminal targets. Hackers have already devised many tricks to lure online shoppers into the game.

It all starts the moment you enter key search phrases like “cheap deals for smartphones” or “best mobile phone deals”. The same goes for cheap holiday packages. Online security solutions firms say that if you have clicked on certain links and answered a few queries online, you probably might have given out details of your credit card or online banking PINs.

“The stolen data may lead to the launch of more damaging attacks or may be sold underground. Cybercriminals used to frequently lead Black Hat search engine optimisation (SEO) attacks against unsuspecting users,” Amit Nath, Country Manager (India and SAARC) of Trend Micro, a global internet security provider, says.

According to Nath, attacks could happen in a number of ways. Black Hat SEO (search engine optimisation) attack is one such possibility. In this scenario, search results for hot items such as gadgets and holidays can be poisoned to lead users to malicious sites.

Another technique is promo scams. Users are lured into malicious schemes whichlook so original and genuine that people have no reason to doubt them. “An example of this is a spam run which we recently saw leveraging Black Friday,” he said.

Session hijacking is also becoming increasingly common. Online shoppers, who are connected to unsecure networks, put themselves at the risk of being exposed to sniffing. Criminals are able to sniff out personal information which allows them to impersonate the user on different platforms, causing financial loss.

Some of the recent attacks noticed by Trend Micro researchers include buying cheap iPhone 4S handsets. The firm found a phishing attack that specifically targets users who are want to purchase an iPhone 4S through e-commerce sites.

“The attack involves domains that display replicated posts for iPhone 4S units. The prices on the fake sites are also dramatically cheaper. You'll also notice that the post cybercriminals have chosen to replicate is one by a seller with a good reputation, in order to gain the trust of potential victims,” Nath says.

Bank alerts

With complaints of online financial fraud rising, banks have begun to send mails to their customers, warning them about sharing information. “Never provide sensitive account information like your PIN, password, account number or personal details in response to an e-mail. If you have entered such

information, report it to us immediately," ICICI Bank asked its customers on Saturday. Other banks too are constantly advising their customers to do the same.

Spear attacks

According to Govind Rammurthy, Managing Director and Chief Executive Officer of eScan, hackers are using what he terms 'spear phishing mails'. They send out mails with laced attachments.

"Unlike mass phishing attacks, a spear attack is targeted at a particular organisation or those using a specific service. For example, a website imitating your regular bank would send you mails requesting your login credentials," he said.

"Users hold the key here. If they fall for the offer and interact (responding by opening the attachment or filling up empty fields), the spear phishing attack is successful." he said.

Rammurthy also says that credit card hacking is synonymous with phishing attacks. Apart from the basic version of seeking credit card information through mails, they sniff out credit cards using skimmers.

Skimmers are card readers which are camouflaged and attached to ATM machines and other routine card swiping machines at hotels and retail outlets. When users swipe their card in the slot, the skimmer reads the magnetic strip data and which is then stored or transmitted via Bluetooth to the attacker, who is usually nearby.

Users may not even be aware of this clandestine activity as the transaction happens normally.

Facebook scams

At the Russia-based Internet security solutions firm Kaspersky Lab researchers found a different method being used by hackers.

Mr David Jacoby, a security expert at Kaspersky, found that cyber criminals impersonate themselves as the Facebook security team after hijacking users' accounts. They then send users an online application to 'reconfirm' their account details, including password and credit card details. The attackers also use the stolen information to log into the person's account and swap their profile picture with a Facebook logo and change the name to 'Facebook Security'. "These scams are just getting more popular and we really recommend not giving out personal information, over social media," Jacoby said.

Ultimately, it all boils down to the basics of security to checkmate cyber criminals. Don't open suspicious looking mails. Don't answer queries from unauthorised persons. Don't click on suspicious links in mails even if you get them from your friends and family, for their accounts may have been compromised. Clicking on such links actually 'welcome' hackers into your system. You'll end up sending back information to hackers sitting thousands of miles away. Some of the links can install 'key loggers' in your system and deploys applications that let people to view whatever you type and take control of your systems.

Don't be under the illusion that it won't happen to you.

kurmanath@thehindu.co.in

Keywords: Online fraud, e-commerce, phishing