CYBER CRIME

The Infomation Technology (Certifying Authority) Regulations, 2001

The Cyber Regulations Appellate Tribunal

Navigation

Cyber Crime Branch Advisory
The Nigerian Scam

Important Links
- Cyber Crime Investigation Cell
- Delhi Police
- Delhi Traffic Police

Phishing in people's accounts

14 February 2007

Today, 10 times more Indians use the internet for their banking needs than five years ago. And not surprisingly, the number of fraudsters eyeing your account have also multiplied. Globally, $6 billion is stolen from consumer accounts by attacks called phising and the scale of such fraud in India is fast catching up.

Sukhwinder Singh can never forget the day he checked his account online in late october last year. His account showed a deduction of Rs 41,000 and he had no clue where the money had gone. Investigation revealed the money had been transferred to one Harpreet Chohan in Delhi. It was later revealed that Sukhwinder had been a victim of a phishing attack on ICICI Bank. He had given his password and name online by replying to an email sent by the hackers. The hackers then logged into Sukhwinder's account and put in their mobile number instead of his. So that, when they did make the transfer, the message alerting Sukhwinder of the transfer would go out to their mobile and not his. This very move proved to be the hacker's nemesis.

The alleged phisher, Harpreet Chohan told CNBC-TV18, "I don't know how the money got into my account. I don't know how to operate a computer, so how can I be a hacker."

Cyber security expert, Vijay Mukhi says, "Phishing normally begins by you getting an innocuous e-mail - let's say from the bank - saying that someone is trying to hack into you account so you need to re-give us your password. So, you click on the link. That website is a fake or the spoofed website. Here you actually key in your personal details - you key in you name, your password when you click on ok, you don't realize that your user name and password has gone to the phisher."

Once the password and user name are with the phisher, it's only a matter of a few minutes before your money is transferred from your account to the phishers. What's even more threatening is that a phishing attack can be launched sitting in any part of the world. Mukhi says, "The problem with the internet is that it doesn't recognize geographical boundaries. So, today most of the phishing attacks to a bank will never occur from the country itself. I would launch a phishing attack on an Indian bank sitting in America and the spoofed page might be in Taiwan."

Finally, when the authorities do catch on, often the money trail leads to empty bank accounts with the cash long vanished. What's more, the attacks have just begun - October has seen over 26,000 phishing attacks worldwide, as compared to 15,000 last year. But industry experts say banks and customers both are catching on at a fast pace.

Head of Operations, ICICI Bank, Madhabi Puri Buch explains, "The interesting trend we are seeing in the case of phishing is that, while the number of attempts being made is increasing, the impact of each of these attempts is sharply declining. Aand the reason is very simple, just as the fraudsters are trying many things - both the banks and the customers come together to find ways to react to these attempts very rapidly. And in today's environment, in just a matter of four hours, these malicious sites are clamped down and they have no impact whatsoever on the customer."

Banks across the country have put up alerts against phishing e-mails on their websites and many have even launched campaigns to alert investors against it, so is this a sign of the increasing vulnerability of the industry?

Buch says, "When you see the tip of the iceberg is when you have to take action - not when you crash into the iceberg. Since, we believe that customers have such a vital role to play in prevention of fraud - not only in the case of phishing but in all types of financial fraud - we believe that it is part of our duty as a very large player in the financial system to create that awareness amongst a larger and larger set of people."So, just how does a phisher launches an attack? Well, you can't see them..or even hear them but sitting behind computer screens, they are plotting their next move to get to your money. Launching a phishing attack often takes just a few hours and just about anyone can do it.

But experts say the sheer ease with which phishing can be executed is threatening as the knowledge on how to launch a phishing attack is often just a click away. Head-S-E Asia & India, Websense Inc, Surinder Singh says, 'It's getting more and more organised by the day. There is a whole set of an organised economy - where there are websites which sell these phishing kits. With these phishing kits, even a layman like me and you without any technical background, can launch these phishing attacks. In one or two days, there are hacking tools which are sold over these websites. It's very well organised and getting bigger by the day."

Experts say phishers often meet in online secret chat rooms and trade knowledge on different security systems and new ways of launching attacks across countries. Mukhi explains, 'Once I was at a chat show on the internet and there were some phishers who were sharing ideas and they were all very unanimous - that most of the banks in India do not have an emergency response team for phishers and they don't respond as fast as an American or European bank would. So, phishers are now going to target Indian banks because they get more user names and passwords than any other banks."

Buch says, 'We have created a special place where an alert can be given and we have found that the speed of response is extremely high. Within half an hour or a couple of hours of the mail first reaching us, we get an alert. The authorities have been extremely helpful. Through the authorities, we are able to bring down the site and there is no damage done to our customers. We are available to our customers 24x7 on so many channels. The people who are mapped to that e-mail ID that I mentioned - in addition to the executive director, it goes to a host of people who are on duty and on call 24x7.'

Sounds far fetched? Not really. Just a few days ago, UTI Bank was the victim of a phishing attack. The Delhi police has arrested four Nigerian nationals and an Indian in the case. According to the police, Oxabe and his accomplices allegedly sent e-mails that included a hyper-link within the e-mail itself. A click on that link took the recipients to a web page which was identical to UTI Bank's site. After the customers had logged in with their passwords and names, the information was sent to the alleged fraudsters who then used the information to transfer large sums of money to various accounts, all over the world, using the internet banking facility.

The police believe it's an international racket involving even more people, sitting in various parts of the world. Additional Commissioner of Police, Delhi police, KK Vyas says, 'They had organised this racket in which they actually sent phishing mails using UTI Bank's details. They had copied the UTI logo etc and on that basis, they prepared letters as if they had originated from the bank.

But phishing attacks are continuing unabated. Last month, UTI Bank filed an FIR with the Delhi police after it received complaints from customers that cash had been debited from their accounts without their knowledge. Customers from Thane, Delhi, Vishakapatnam, Nasik and Ahmedabad - all had one thing in common- they had replied to an e-mail from the bank.The damage: 30 customers who lost Rs 20 lakhs and this amount was reported by the ones who caught on early.

KK Vyas explains, 'We had been receiving more and more complaints and that means this scam could run into a very high proportion. It is quite possible that other branches of UTI Bank in various parts of the country might also be affected. So, the process of verification is going on and we are in the process of identifying where all the money has gone.'Data from the Computer Emergency Response Team India shows phishing attacks are on the rise. The year 2005 saw 86 incidents of phishing reports. In 2006, this number more than doubled to 200 incidents. Not only were attacks being launched in India but 2006 saw the maximum phishing attacks being launched from India on other countries as well.

Security expert, Surinder Singh says, 'As per Websense Security Lab, we find that at any given point in time in 2006, there were 2 to 300 websites being hosted. There was a spurt in October where we identified 790 websites which were hosted in India and being used to carry out attacks."

Buch adds, 'Over the last six months, we have done three specific initiatives. We introduced true factor verification on the website, which means in addition to the user ID and password, the customer now has a challenge mechanism, where we ask them things only they know and only if the answer is correct, do we allow him to do a transaction. '

But Singh admits, 'No system is perfect because all these criminals also study what protection techniques are being used and they will come up with something new. It's kind of a guerilla war. You can limit the phishing incident, so you can reduce the exposure but there's no way of totally eliminating it."

Phishing and phishers may be keeping banks on high alert but the law is lagging far behind. Cyber Law expert, Pawan Duggal explains, 'Phishing is not an offence that is specifically defined under the IT Act, 2000. The law enforcement authorities are keen if at all to report and register a case under the typical generic provisions of cheating and criminal breach of trust under the Indian Penal Code, IPC.'

One of the bigest problems when you encounter phishing is that of cyber jurisdiction. Since these attacks are launched from any part of the world with the victim in a separate country, prosecutions of such cases becomes even more difficult.

Duggal says, 'One of the biggest problems in phishing is how do you go ahead and arrest these kind of offenders. If you look at the law book, it gives you an academic answer. The IT Act, 2000 has extra-territorial jurisdiction and it applies to any person of any nationality anywhere in the world - so long as the impacted computer is physically located in India. But having said that, the reality is that the Indian law is still not applicable to people outside the territorial boundaries. Therefore, the law enforcement agencies reach a dead end.'

With the loopholes in the law, the best way to keep your money safe is to protect yourself from such attacks. Here's how to do that:

- Be on the alert when a banking e-mail uses dramatic information to get you to react immediately.
- Be ware of e-mails from shopping websites offering free goods. It might be a scam to get your banking details.
- Phishing e-mails are not personalized. Your bank will generally use your name when they contact you.
- Finally, clicking on phishing sites may install a spying device on your computer. Downloading an anti-spyware programme will help.

Buch adds, 'We believe that working together with an alert set of customers and with banks who take very rapid action is the perfect antidote. With the authorities coming in and catching and penalizing the offenders, this combination is very rapidly going to make it not worthwhile for a fraudster to even attempt it.'

India is at tenth place when it comes to hosting phishing sites with the US and China biting the phishing bait more often. The United States remains at the top with 28.78% of all phishing sites located out of the United States and 11.96% out of China. Korea, Germany, Australia, Canada, Japan, United Kingdom, Italy and India are the other countries where phishing attacks are prevalent. As of now, 2.11% of the phishing sites are located in India.

Singh says, 'India on the threshold of having more and more people getting into online banking or taking online peronal loans. So, it won't be a surpirzse if someday someone tells me that out of the total size of frauds happening - India would be at 1% or 2% - but even that would be Rs 200 crore."

Though Buch says, If you look internationally at any of the large 3-4 banks in the world, they would be experiencing one phishing attempt a day. We are nowhere near that number.'

But even as banks are gearing up to tackle phishing, there is another kind of threat emerging - phishers are trying to get account details over the phone and this is called wishing. Singh explains, 'Instead of phishing, it's something called 'wishing', where they are using VoIP. Banks are telling people not to click on links. Now e-mails are coming saying that call us on this number for some particular reason and when people dial that number, actually it's not going to the interactive voice response or IVR of the bank, it's going to some other IVR, which mimicks the IVR of the bank and you are asked your credit card details or

some other details. So, new ways will keep coming up." Mehak Kasbekar

India Cyber Law and Cases

Welcome to the largest Database of Cyber Law and Cases from India. We publish cyber law cases & news from India. Send your suggestions / articles / news

read more

Latest News

20 November 2010

30-Month Sentence For Bot Nets Used To Obtain Information From Other Computer Systems

19 October 2010

Computer Specialist Pleads Guilty to Securities Fraud Committed through Hacking, Botnets, Spam and Market Manipulation

read more