SMS phishing on the increase

Companies that communicate with their customers using SMS could leave those same custome wide open to phishing, the fraudulent attempt to collect personal or banking details. Companies need to ensure that their customers are made aware of the types of SMS messages they send out, and what, if any, information they might request via the SMS channel to reduce the risk of SMS fraud through phishing attacks.

By Dr Pieter Streicher 3 Jul 2008

Technology is used to protect people and companies against fraud but unfortunately it can also be used t assist fraudsters during a scam, especially when certain technologies are used widely among businesses send communications. Increasingly, reckless communication practices by companies play into the hands fraudsters. All it takes is one irresponsible communication that fraudsters can replicate and a company's integrity will be at risk and its customers' defrauded.

This is true for email where the most common techniques used to defraud people are phishing scams, an attempt to trick a person into revealing personal information such as credit card details or bank account information by sending an email with a fake web address or telephone number, and ‘419 scams', so name after the section of the Nigerian penal code that addresses fraud schemes, where a person is persuaded advance relatively small sums of money in return for larger financial gain.

Due to the broad appeal of SMS for business communications, phishing scams now also target cellphone users by using an SMS to initiate a communication.

SMS phishing, or “smishing”, occurs mainly when customers receive an SMS from what seems to be a reputable financial institution prompting them to call a telephone number due to a possible fraudulent transaction on their account. They are then requested to divulge their bank PIN number, or other personal details, on the pretence of changing their PIN to securing their account. The fraudster however is now able to access the callers' funds. Customers are a victim of the very fraud that they were trying to prevent when they were proactively following up on the SMS.

The communications conundrum

While SMS messaging can be used in many ways to make transactions safe and reliable, it requires the careful planning and the implementation by companies of suitable communication policies and procedures Companies require a good understanding of the benefits of SMS in that messages are read immediately a people have cellphones with them all the time. Companies also need an understanding of SMS's

weaknesses, in that messages are not encrypted and are easy to imitate.

Some banks even perpetuate the impression that it is acceptable to divulge your personal information via insecure electronic channels - as long as you provide it only to your own banking institution.

For instance, a South African private bank credit card guide encourages their clients to request electronic statements by emailing their name, credit card number, ID number and preferred email address to the em address or call the client care centre telephone number provided.

Not only is email an insecure means to send personal information but fraudsters can quite easily pretend t be your bank and imitate marketing material, emails and SMS communications. Phishing scams go so far t disarm customers by including the warning: “don't divulge your personal information to anyone but your trusted bank” in an email sent to a bank's client.

Then there are your typical SMS banking notifications telling you that someone has logged onto your Interr banking account. The bank's name is followed by: “Internet - confirmation of log on: Account number endi in …5601: 26June08: 17h45: Helpline: 021 xxx xxxx”. As SMS messages are plain text, it is very easy for fraudsters to imitate this message and include their own contact numbers in a message.

In addition, by sending you this message, you would suspect that someone has fraudulently logged onto your Internet bank account. You call the number displayed in the SMS thinking it's your bank's call centre, and there is someone on the line that asks you for all your relevant personal and account details and then offers to change your PIN to ensure the security of your account. At that point you have given all your account details and are now open to fraudulent activity on your account.

While it is easy to get caught up in the threat of SMS phishing scams, the most effective solution to comba this fraud is for businesses to educate their customers about the risks involved when responding to an SM Fraudsters rely to a large degree on the ignorance of people and the trust customers place in their bank o another reputable brand.

Tips for businesses

1. Only send out relevant information and never ask customers to provide sensitive information via insecure electronic channels such as e-mail or SMS.
2. When communicating with customer using SMSs, personalise the messages and include information that would not be available to phishers. This will enable customers to distinguish between legitimate a phishing messages.
3. Look critically at your SMS and email communications, and consider whether fraudsters could benefit from imitating your message. Educate your customers on potential phishing scams. Inform your customers as soon as you are aware that someone has been using your company name fraudulently.
4. Make your SMS messaging policies known (i.e. message will always be personalised or we will never ask you to give us your PIN number).
5. Ensure that your marketing material is consistent with the communications you send to customers and that call centre staff are well-trained.

Tips for customers

1. Never respond to an SMS or email message that requests personal information. Do not divulge sensitive information such as credit card numbers via insecure electronic channels such as SMS, em or over the telephone.
2. Be aware that it is easy for criminals to imitate organisations by using electronic communications and initiate emails or SMS phishing scams. If unsure whether or not something is a scam, always take the time to investigate it.
3. Always verify a contact number, especially those in emails or SMS messages. If the “bank” called yo call them back. Double check phone numbers that appear in an SMS - you can do this via the Internet by referring to any marketing material. For ease of reference, store banking phone numbers on your mobile phone, along with email and website addresses.
4. Never ever give your PIN number or password to a PERSON. Only use your PIN on systems that hav been designed for this purpose, i.e. ATMs and official Internet banking sites. These systems have been designed such that employees at the bank cannot access this information.
5. Report it. If you are unsure of how a company received your number, or are suspicious about an SMS that you have received, you should contact the company and report your concerns. You can also repo an SMS scam to Wireless Application Service Provider Association (WASPA) (www.waspa.org.za, th industry body that handles all complaints relating to commercial messaging in South Africa.

ABOUT DR PIETER STREICHER

Dr Pieter Streicher, MD of BulkSMS.com (www.bulkSMS.com), graduated from Wits University with a BSc-Eng (Civil) in 1991. In 1996 he received his PhD from UCT. He worked as a ci engineer for four years at HHO Africa. In mid-2000, Streicher, along with Richard Simpson, [BSc-Eng (Civil), MBA], established Celerity Systems. BulkSMS.com was set up as a division Celerity Systems to focus on SMS solutions for business and mobile users. Today, the Cape Town-based company is a leading wireless application service provider offering services nationally and internationally. Pieter is active in the Wireless Application Service Provider Association (WASPA) and sits on the WASPA working group addressing national regulatory issues. Contact him on +27 (0)21 552 6321 or email info@bulkSMS.com.
View my profile and articles...