LIFE Strategies TODAY

March 2015

Fraud via Mobile Phone Porting

This topic has been on our list of things to share with you via our regular newsletters for some months and has finally made it to the top of the list after one of Life Strategies' valued clients experienced mobile phone porting in the last couple of weeks. We take the opportunity explain what happens and what to watch out for.

Our client received a notification that his mobile service was being moved to another provider. He immediately called his bank to have his accounts temporarily blocked. He then contacted his phone provider and also notified Life Strategies.

Life Strategies assisted with contacting various providers who disabled online transacting. Fortunately no fraudulent transactions took place. The inconvenience though was not inconsiderable - a few days without a working mobile phone until the number was ported back to the correct provider. Also, to have online transacting restored, he was required to prove to institutions that a full computer scan had been completed.

What is Mobile Phone Porting Fraud?

As more of us use our smart phones to access our bank accounts and conduct on-line transactions, fraudsters have been quick to exploit the banks' two stage SMS security mechanism that requires you to authenticate any transfers to an account you have not previously transacted with.

If you have changed your mobile service provider and kept the same number you would also have arranged 'phone porting' to your new supplier.

Fraudsters are increasingly employing mobile phone porting as a sophisticated new means to steal your mobile phone number, then instigate and intercept your bank's online verification code that allows them to transfer your account balance into their own.

Warning sign

Your mobile phone service has been disconnected suddenly or you are notified of a change in provider.

What should you do?

- Immediately call your mobile phone provider to find out why your service is being transferred or is no longer working.
- If your service has been transferred, contact your bank(s) as soon as possible, advise them of this potential porting, and have your bank discontinue your on-line SMS authorisation service until the situation has been rectified.
- Call Life Strategies. Our team will arrange to notify providers of any accounts we assist with.

The Scam

Following is a real-life example on how phone porting ID fraud is achieved; only the names have been changed to protect the privacy of those involved.

Joe is a small business owner who was justifiably alarmed after receiving an unexpected call from his bank on his home phone. The bank's bad news was that his mortgage account had been accessed and $45,000 stolen by fraudsters. He also learned that his mobile phone and the bank's SMS payment authentication system were used to complete the fraud.

Joe had assumed that his money could not be transferred to an account he had not previously transacted with, without first entering the authentication code his bank always sent an SMS to his mobile as a secure way of verifying payments.

SMS authentication is a popular form of two stage security authentication that most banks use to verify approval when a customer uses online banking to transfer significant amounts of money to an account that has not previously been transacted with.

When a customer creates a payment transfer to a new account, makes a large payment or purchases something from selected online shopping websites, the bank automatically sends an SMS verification code to the account holder's mobile number. The code is then entered by its recipient into online banking as a way of confirming that it is the bank's actual customer using their online banking service. Foolproof you would think, however when fraudsters took the $45,000 from Joe's account, they also had control of his mobile phone.

So how was it done?

In the days leading up to the fraud being committed, Joe had received two unusual phone calls. The first was to Joe's office, from a caller claiming to be a representative of the Australian Tax Office, simply confirming that Joe still worked at the company. Three days later a second call was received on his home number, during the day when Joe was predictably at work. Joe's daughter answered the phone, and without thinking twice provided her father's mobile number plus some basic personal information to this second caller who posed as one of Joe's clients trying to confirm arrangements for an urgent job.

The fraudsters used this information to contact Joe's mobile phone provider and request that his phone number be ported to a new device. If your online banking credentials have been compromised, scammers may transfer your phone number to another provider so they can receive security codes sent by your bank.

Now armed with some basic banking details and Joe's phone number ported to their own mobile, the fraudsters accessed Joe's online banking service and requested that the $45,000 deposited in his mortgage account be transferred to their own. Joe's bank then automatically sent an SMS verification code to Joe's ported mobile number, allowing the fraudsters to simply enter the bank's authentication code as Joe's genuine online transaction confirmation.

Should you continue to use online banking?

Like you, we appreciate the convenience of online banking however we stress to all Life Strategies clients that even with the banks' SMS security process as a way to authenticate payments, the system is still reliant on your easily accessible mobile phone number.

Therefore, please remain vigilant just in case your mobile phone service is disconnected suddenly, or you are notified of a change of provider; this could signal that your phone number has been fraudulently ported.

(Part of this article was originally published by Bankwest)

Update on Training Attended

Sharni

11/3/2015 – Farrelly's Dynamic Asset Allocation – looks at forecasting investing (securities and commercial property returns) over 10 years,

6/3/2015 – Ethics training requirement – case study in Taiwan's credit card crisis,

17/2/2015 – Portfolio Construction Forum – Markets summit

12/2/2015 – The Tax institute TASA and the TPB Code of Professional Conduct – competency exam.

Michael

12/2/2015 – Completed the FPA Life Risk Specialist program

12/2/2015 – The Tax institute TASA and the TPB Code of Professional Conduct – competency exam.

Jo

10/3/2015 – Attended the BGL Simple Fund Update Seminar

New and improved newsletter format

You receive our “Life Strategies Today” newsletter quarterly, which provides general interest topics such as travel money or internet fraud plus regular articles on mortgage rates, tax changes, insurance case studies and updates on what our team have been doing.

We are trialling a new shorter format for our newsletter, which will now be sent monthly. We hope you will continue to find this of interest.

The newsletters continue to be available on our website:

http://lifestrategies.net.au/news-events.

For questions or general feedback about our newsletters or the new format, please contact us at: yourfinancialcoach@lifestrategies.net.au

Facebook Google Plus LinkedIn Our Website