Alert: How you can be scammed by a method called SIM Splitting

The National Fraud Intelligence Bureau (NFIB) is reminding the public of a method called “SIM Splitting” used by fraudsters to steal your money.

How the scam works
Organised Crime Groups (OCGs) in the UK purchase victims’ personal details that are obtained through the spread of Trojan malware. Victims’ detail packages are purchased from overseas OCGs specialising in the collection of compromised personal data to sell. Specific data is extracted, namely online bank account details and statements. Using the victim’s banking details to gain telephone access to the bank account, the fraudster then opens a parallel business account in the victim’s name. Opening a business account is subject to less stringent security checks once an individual already has a current account with a bank and helps make any transfers of money in the future less suspicious. Details of the victim’s mobile phone, again extracted from the purchased personal data package, are then passed to an individual who specialises in the SIM Split step.

This SIM Splitter then:
- Uses the bank statement obtained through the hacking to establish the mobile network the victim belongs to;
- Uses open source searches, using the victim’s details, to ascertain potential answers to security questions;
- Uses open source searches to establish the mobile phone network provider;
- Obtains a blank SIM card, either through an insider at a phone company or by purchasing one;
- Contacts the phone provider and tells them that the mobile phone has been lost/damaged.

The new SIM card is activated while the victim’s is cancelled. Contact details and security questions may be changed with the phone provided to further hinder the victim from reporting the fraud. As soon as the SIM card is activated, the SIM Splitter contacts the OCG and tells them to transfer funds from the victim’s current account into the newly set up business account. As a security measure the banks will often make a call or send a text to the phone number registered to the account to confirm if the transaction is genuine. The SIM Splitter agrees to the transfer when contacted and disposes of the SIM card afterwards so not to be traced. The OCG can withdraw or transfer funds away from the business account with a lower level of scrutiny whilst maintaining a certain level of access and control of the account with the stolen details.

How to protect yourself against this type of fraud
- Always make sure you have suitable anti-virus software installed and that your firewall is switched on.
- Always consider what you are downloading – do not open files from unknown sources.
- Be wary of ‘pop-ups’ requesting unsolicited downloads.
- If you discover a virus on your computer, disconnect from the internet immediately and ask a specialist for advice.
- When creating a password, try not to use the same password for more than one account. This will prevent further accounts being taken over if one has been compromised.
- Use complicated passwords: vary the case, use 8 or more characters. Never use personal information such as names or dates of birth.
- Try not to post information on social media such as your birth date, your first pet, or school as these are normally included in security questions to reset your password. Fraudsters may use these answers to access your account via the “Forgot Password” link.
Feedback

The NFIB’s Proactive Intelligence Team conducts debriefs with convicted fraudsters and passes the sanitised information direct to industry and the wider community. Any questions regarding the content of this alert can be sent to:

PIT@cityoflondon.pnn.police.uk

The ECD needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following ECD feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU. This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send this to NFIBfeedback@cityoflondon.pnn.police.uk

Copyright © City of London Police 2015

NFIB Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this Alert, it is provided in good faith on the basis that the Commissioner, the City of London Police and its police officers and staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to the City of London Police. Should you or your police force hold information, which corroborates, enhances or matches or contradicts or casts doubt upon any content published in this Alert, please contact the City of London Police NFIB by return.

Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.