BARCLAYS

Protecting your business from Social Engineering and Cyber Fraud Threats

Social Engineering Threats

Fraudsters have long identified that the easiest way to breach an organisation's defences is to target people, not systems. Social engineering is the manipulation of situations and people that results in the targeted individuals divulging confidential information. This can be through a social media site, email or the phone.

To mitigate the risks, consider raising awareness on a regular basis amongst your staff, customers and suppliers of the following prevention measures:

- Think about social media networks and your website – it is vital that staff do not publish personal details, such as date of birth, role details or other employment information either in their profiles or in posts so that these are not readily available for fraudsters to use
- Avoid sharing the movements of senior staff on social networks or your website – this may seem harmless but can help fraudsters use this information to impersonate them
- Access the guidance that most social media sites offer on online security including privacy features to restrict access to your profile and be careful about who you let join your network
- Do not click on links or attachments in unsolicited emails or text messages even if appearing to be from a known sender, such as your bank or social network site; always access sites through known and verified links or go to the company's website using an internet browser
- Be cautious of unusual emails external to or within your organisation, such as payment requests, a change of bank details, or a request for personal details.
- Fraudsters use technology to replicate genuine email addresses and telephone numbers to reassure potential victims. Always independently verify any request
- Do not respond to unsolicited phone calls even if the caller appears to be from your bank and has relevant information about you or the business. Wait ten minutes and call back from an independently verified number or one that is already known to you
- Always challenge giving out personal or financial details to anyone without independent verification, regardless of who they are.

The cost of fraud to the UK economy is £52bn[1]

The cost to the Private sector is 21.2bn and £20bn to the Public sector[1]

There are 36,600 organised criminals[2] in the UK

Internal fraud will cost a business around 8 times more[4] than external

1 in 4 businesses has been the victim of fraud[1]

37% of organised Crime Networks commit fraud, approximately 5,300 groups[3]

[1] National Fraud Authority (NFA) Annual Fraud Indicator June 2013.
[2] The National Crime Agency 2014 Strategic Threat Assessment of Serious and Organised Crime.
[3] Metropolitan Police "Little Book of Big Scams Business Edition" 2014.
[4] 2012 Audit Commission report – Protecting the Public Purse.

Cyber Fraud Threats

Social Engineering can be the enabler to Cyber Fraud. This can occur when malicious software (malware) programmes infiltrate, corrupt and steal information such as log-in or personal details from computer systems, which are then used by criminals to obtain the victim's money.

To mitigate the risks, consider raising awareness on a regular basis amongst your staff, customers and suppliers of the following prevention measures:

- Ensure that all sensitive information and files are backed up on external devices disconnected from a network or the internet
- Install and regularly update anti-virus/anti-spyware software on all systems and ensure firewall settings are up to date and set to the highest protection level

- Consider using a dedicated computer for your payment transactions, reducing the risk of exposure to malware
- Treat your smart card in the same way as your debit or credit card. Once used, remove the smart card from the card reader (even while still logged in) and keep secure at all times when not being used to sign a payment or perform an administration change
- Always log out from payment systems, such as Barclays.Net, remove your smart card and store it securely. Never share smart cards or PINs
- Memorise your PIN and do not allow your web browser to remember details of the PIN
- Use dual authorisation where possible. For example one staff member can input payments on a machine and then a second staff member should check these before authorising on another machine. Reconciliation should be carried out regularly
- Immediately report unexpected behaviour or screens that are not usually displayed to you internet banking help-desk and do not use your internet banking. Keep up to date with the latest social engineering techniques and malware threats by visiting www.getsafeonline.org.

To find out more about managing fraud in your business, please speak to your Relationship Director.

Social Engineering Case Study

Company A had recently engaged with a new Public Relations company, and one of the suggestions made by the PR firm was that Company A should present a more public face to their clients. As a result, Company A put information about the business and their senior people onto their client-facing internet site, including the company structure and senior managements' biographies. The company's senior management also wrote blogs about their travels and activities within the business.

Shortly afterwards, the accounts team started to receive calls from the CEO of Company A. The CEO stated that he was travelling in Europe and that the firm had become involved in litigation with a supplier and, while it was unlikely, an adverse court outcome may require them to make an urgent payment.

The calls continued over a number of days, during which time the CEO provided more information about himself and expanded on the litigation issue. On or around day five, the CEO called again, and advised that the verdict had gone against Company A. He stated that a payment was required immediately to the court, and failure to make the payment that day would result in an increased fine. Payment details were provided to the accounts team and the payment was made, for the sum of £250k.

It was later revealed that the payment was fraudulent; the caller was not the CEO and the information about the CEO and his whereabouts had been taken from the internet. This cost Company A £250k simply as a consequence of a few telephone calls.

www.actionfraud.police.uk