CARDNET

Cyber smart payments update

Understanding hackers to protect your business from fraud

LLOYDS BANK

This White Paper harnesses the knowledge of leading experts in the field to help you understand a hacker's mindset, so that you may enhance your company's ability to defend itself against this rising threat.

Developing better defences

A growing number of businesses, both large and small, are finding themselves under attack from cyber criminals. No company can afford to be complacent. Some hackers work alone but much of the threat comes from large teams operated by organised crime gangs across the globe. In the world of cybercrime, there are no borders and no target is completely off limits.

Understanding tactics

To prepare for the possibility of a cyber attack, you first need to understand something about the tactics used by hackers. All attacks exploit some kind of vulnerability but exactly what those weaknesses are can vary greatly depending on the size, nature and sophistication of a business. Some hacking tactics are completely indiscriminate; others are carefully tailored for a specific target. And while it's already clear the problem is growing, we are likely to hear about many more UK cases from May 2018 when reporting of breaches involving personal data is due to become mandatory.

Cybercrime: Six key points

64%

increase in fraud offences related to UK payment cards between 2011 and 2016

Source: ONS

£6 in every £10

of attempted fraud is prevented by banks and card companies

a total of

£678.7m

in the first half of 2016

Source: Financial Fraud Action UK

Nearly

1 in 20

cardholders were a victim of card fraud in the year to March 2016

Source: ONS

$81m

stolen in a cyber heist by unidentified hackers on the Bangladesh central bank in February 2016

In the first half of 2016, card fraud as a proportion of card purchases equated to

8.7p for every £100 spent

Source: Financial Fraud Action UK

A quarter (26 per cent) of people admit providing personal details to people claiming to be from their bank, even if they do not think they should

Source: Financial Fraud Action UK

Be prepared, be insured

Experts are clear that the companies that suffer most from having their defences breached are those that have done the least to prepare for such an eventuality. First steps include ensuring your business's insurance coverage includes electronic crime and considering whether suppliers have any cyber flaws that could compromise your business. When developing new digital channels, it's also important to ensure you have a security expert, either internal or external, engaged in the process.

Know how to react

Good cybersecurity professionals should be willing to discuss your appropriate level of defence without claiming to guarantee you won't fall prey to hackers. Most companies could benefit from having a pre-prepared 'playbook' to guide key people on how to react in different scenarios (see example below). How will you keep customers informed in a fast developing situation? Who will take charge if the Director or CEO is on a plane? Will you be ready for the potential scale and pace of reaction on social media? Planning how to respond to such things in advance can help your company react swiftly. It is also crucial to understand that as well as the immediate effects, cyber attacks can cause significant long-term damage.

"People often see data security as an IT thing. It's not. Data is the lifeblood of business and responsibility for it must sit at board level."

Ken Munro, Partner and Founder of Pen Test Partners

'Beneath the surface' impacts could include:

- Insurance premium increases
- Lost contract revenue
- Reputational damage to your trade name
- Loss of intellectual property

A pre-prepared response playbook can give your company the capacity to minimise damage if an attack does happen.

It can be rehearsed just like fire alarm procedures. It should cover at least four key steps:

- Pulling the plug to stop the attack by taking your business offline
- Asking security experts to identify how hackers gained access to your system and how to fix it
- Ensuring no latent vulnerabilities exist and improving security before going back online
- Maintaining trust with customers by being honest, open and professional about resolving things – managing communications and media is vital

The basics: prioritising the 3Ps

Experts point to 3Ps that represent a good starting point for any cybersecurity review: patches, passwords and people.

Patches
Make sure security and software updates are implemented on all your servers. Hacks often succeed simply due to basic human error – failure to carry out a regular update can open the door to hackers.

Passwords
Hackers frequently exploit blank, common or default passwords to gain entry to a treasure trove of data. Multifactor authentication makes systems more secure. As well as fingerprint or retina recognition, industry experts point to the potential of 'behavioural biometrics' to measure uniquely identifying patterns in how we act. Keystroke dynamics and mouse movement are examples.

People
Train your staff to spot 'social engineering' attempts to glean crucial information on the phone or in response to phishing emails. Cyber-enabled confidence tricks often involve the use of fake company logos and targeting of financial controllers or payment clerks whose details can be found on resources such as LinkedIn.

> "The challenge is balancing the high security customers demand with the ever increasing desire for convenience."
>
> Phil Thomas
> Head of Product, Lloyds Bank Cardnet

A fine balance: security and convenience

Convenience is vital for 21st century consumers and payment innovations have recognised this. But striking the right balance between security and this desire for convenience is a significant challenge. Phil Thomas, Head of Product, Lloyds Bank Cardnet®, said consumers need "behavioural nudges" in order to reach a happy equilibrium.

We recognise that there are no one-size-fits-all cybersecurity solutions. This paper is intended to help you consider what steps your business should take to protect itself.

Contributions from :

David Ferbrache, OBE, Technical Director, KPMG,
Ken Munro, Partner and Founder, Pen Test Partners,
Phil Thomas, Head of Product, Lloyds Bank Cardnet.

Quotes were taken from :

Lloyds Bank Cardnet Cyber Smart Payments Update: A Hacker's View on Payment Fraud, 26 January, 2017

Important Note:

The information shared during our Cyber Smart Payments Update webinar was accurate at the time of recording but many of the regulations we discussed are subject to change.

Lloyds Bank Cardnet encourages clients to remain up-to-date on regulations and we will continue to use a range of communications platforms to help you navigate the changing payments landscape.

For more information visit
lloydsbankcardnet.com

LLOYDS BANK