LLOYDS BANK

School Email Hacking Used to Target Parents

Lloyds Banking Group have detected an escalation of criminal gangs hacking into school email accounts and targeting parents of children attending independent schools in a fraud campaign.

Parents with children attending independent schools are being approached by email which appears to have originated from the school. Payment instructions for school fees are provided, often offering discounts for prompt payment. The beneficiary accounts quoted, direct the funds to accounts under the fraudster's control.

The bank has seen emails received by parents sent from the correct school email address and quoting the child's name. It is possible that the school's email account has been hacked either driven by a password compromise or malware infection.

In these circumstances, it is usually the parent making the payment who will be responsible for the loss. By the time the fraud is identified, in most instances, the funds will have been moved on and cannot be recovered.

Advice for Parents

Schools are urged to alert parents of their pupils and students to this attack. The following advice should also be provided:-

- Always verify an email payment request directly with the school, via the official, established contact details you have or have obtained from a trusted source e.g. phone number obtained from the school website. Be alert to unexpected fee requests
- Do not attempt to verify the instruction by replying to the email or by making contact with a phone number included in the email
- Be particularly vigilant when you are being asked to send payments to new or different bank accounts than those normally used by the school. Check for inconsistencies and grammatical errors in emails, such as a misspelt school name or a slightly different email address; these can be warning signs of fraud. Do not rely on the fact that the school email address appears to be correct

Advice for Schools

- Ensure that you work closely with your IT Security provider to ensure that all software including anti-virus software is up to date. Where software patch updates are received from suppliers, ensure your systems are updated as quickly as practicably possible
- Ensure firewalls are correctly configured and always turned on
- Train your staff to be alert to emails from external sources and not to click on links or attachments unless they are certain that an email is genuine
- Encourage staff to report instances immediately to IT Security providers where they believe they may have clicked on a link or attachment included in a rogue email

- Passwords - ensure staff are using strong passwords to access the school network e.g. three random, unconnected words (not directly associated with the individual – avoid using children or pet names)
- Get staff to change passwords immediately if they believe their password may have been compromised
- Report any instances where computers are running in an unusual manner e.g. slower, noisy or hotter than normal

For further help and support, please contact your Relationship Management team or visit the banks website:
www.lloydsbank.com/fraud
www.bankofscotland.co.uk/fraud

Ian Buss
UK Head of Education
Lloyds Bank