EUGENE F COLLINS

Cyber Crime: How to limit your risk

Cyber Crime: How to limit your risk

Published: 4 December 2018

Eugene F. Collins has in recent months noted increased incidents of cyber-attacks against our clients. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by hackers disguising themselves as a trustworthy entity in an electronic communication.

Business Email Compromise (BEC) is where a hacker sends an email or emails that appear to be from individuals or businesses you know to obtain your bank account numbers, passwords, or in an effort to convince partners or staff of your firm to transfer funds to an incorrect bank account to the criminals' benefit. Between 2013 and 2015, there have been over 22,000 BEC victims in 79 countries, with an average loss of US$3.1bn. Most importantly, BEC attacks are constantly growing and becoming more elaborate. All businesses must act now to protect against such attacks.

Tips to protect your business include the following:

- Provide existing and new clients with your bank details and inform them that your banking details will never change. If they receive any correspondence announcing a change in bank details, advise them to contact you and verify your details before they pay.
- You can consider leaving your bank details off your invoices and call clients to give them this information instead.
- Use colour coding: virtual correspondence. E-mails from employee/internal accounts are one colour and e-mails from non-employee/external accounts are another.
- Change passwords regularly and have an IT maintenance schedule.
- Periodically check email folders to make sure new folders have not been created without your authorisation.
- Communicate early with clients about the best way to correspond with them electronically. Warn them about the need for them to ensure that their email and computer systems are not compromised, and to let you know if that happens, so you can communicate in another way.
- Use trusted anti-malware software.
- Never enter a password or other information on a website clicked in an email. Often, phishing emails are disguised as warnings about your account.
- Never enter a password or other information in a browser unless "https://" appears in the URL in your browser.
- Avoid free, web-based email accounts such as yahoo.com or gmail.com. Purchase a company domain URL and use it to establish company email accounts.

The UK Solution

While the Law Society of Ireland has provided a note on cyber-attacks and the Central Bank has introduced initiatives on cyber security there are no definitive plans to tackle this threat.

In the UK, the Payment Strategy Forum has introduced the "Confirmation of Payee" system which should largely eliminate the very serious risk of BEC. If the account name is correct, customers will receive confirmation and can make the payment. If the name is wrong, they will be advised to contact the recipient to get the correct details.

At present, banks, both in the UK and Ireland, are under no obligation to check the intended account name to be paid, this loophole is working to the hacker's advantage. The new code of conduct in the UK

is now due at the beginning of 2019. If a bank doesn't seek any evidence of Confirmation of Payee, it will be liable for any loss.

It will be interesting to see if Ireland follows suit.

For further information on this topic please contact:

Rachel Shanley
Partner
Dispute Resolution
D: +353 1 202 6556
E: rshanley@efc.ie