SMEs must be aware of salary mandate fraud

This is the first article to be released by the Bank of Ireland's e-crime team. We are hoping to raise awareness on current fraud trends targeting BOI business customers.

What is salary mandate fraud?

Salary mandate fraud is one of the fastest growing fraud types targeting businesses in 2019.

This type of fraud occurs when fraudsters target individuals in an SME's HR, payroll or finance department with the intention of successfully transferring their employee's salary into fraudulent mule accounts. Emails purporting to be from employees are sent to these departments, requesting a change to the account details the salary is mandated into each week/month. HR staff, if tricked, will then complete the request and funds will be transferred to the fraudster's account. In most cases it is a number of days before the staff member realise, giving the fraudster enough time to "cash out" the fraudulent funds.

Who can be targeted?

Every business is a target for this type of fraud. Smaller operations with local HR teams (or individuals) will be most vulnerable to this type of attack. Fraudsters will pick their targets carefully and carry out significant reconnaissance before launching their attack. Information for most businesses is more publically available than people realise. Social media, especially LinkedIn, Twitter and Facebook are great for promoting your business but have their own risks. A lot of information is posted online and this makes these attacks easier for any potential fraudster. A lot of businesses publicise HR staff names and email addresses on their own website – making this easier again for criminals.

How this fraud can occur?

- An internal department within a business (usually HR) receives a simple email from an employee asking can salary be changed from one account to another
- This email might contain a reason such as "I need to change it for my mortgage"
- The HR staff member makes the change on the payroll
- When the next payroll batch is processed, the salary is redirected to the "new" account
- The employee will notice first they haven't been paid
- In a lot of cases the funds will be moved on or cashed out immediately

Examples:

Prevention – STOP and THINK

- Confirm the request! Keep up to date contact details for your staff – a quick phone call confirming any amendment will stop this type of fraud.
- Increase fraud awareness with frontline staff, something as simple as an agenda item at the monthly meeting.
- Consider running ethical phishing campaigns. There are lots of vendors who offer this service
- Ensure there are adequate controls in place in HR and finance departments – a “four eye” check on any account changes is an effective way of mitigating this fraud type.
- The security zone page on the Bank of Ireland website has lots of information for business customers, including current trends. It’s a good idea to keep up to date with industry awareness groups like Fraud SMART (ROI) and Take Five (NI/UK) for the latest trends and safety messages.

Published by Stephen Larkin on behalf of Bank of Ireland's e-crime team

Published: 7 November, 2o19