30th March 2024

AIB urges businesses to exercise caution as fraudsters seek to take advantage of busy Easter payments and tax period

Email scams and investment fraud popular as tax year ends for many businesses

AIB launches fraud campaign to help businesses spot the signs and stop fraud before it happens

AIB is urging businesses to exercise caution as a number of scams are in circulation, with criminals seeking to take advantage of the busy Easter period for payments. The two-week period over Easter is typically a busy time for businesses when it comes to payments as it is the end of the tax year for many and it's the end of the quarter. Fraudulent invoice redirection or email fraud, investment scams and malware are threats that are particularly prevalent. AIB is launching a new campaign to help businesses spot the signs and stop fraud before it happens.

Invoice Redirection or Email fraud

Criminals hack directly into company email accounts or create new ones that are almost impossible to tell from the real thing. They email staff members posing as their manager, instructing them to urgently transfer money to a new account. They also pose as suppliers asking staff to change their payment details. Businesses are urged to ensure that all staff are aware of this threat and are reminded that when it comes to making payments or transferring money, never act on email instructions alone. Instead, talk to the person directly on a trusted phone number to check if the request is real.

Investment scams

Investment scams are highly sophisticated and experienced business people can be taken in by criminals advertising them online. Criminals create fake websites promising far higher returns than usual. The websites will always have a page that looks for contact details to allow criminals make their first contact with you. They will call or text from numbers that look genuine and often supply high quality brochures. Business people are urged to remember that if something seems too good to be true, then it probably is. Always check that a firm is regulated and check that the person you're talking to really works there. Always look for independent financial advice and don't be pressured into making urgent payments.

Malware

Businesses are also reminded that criminals can make fake bank websites that look exactly like the real thing but which contain malicious software, also known as malware, designed to get

unauthorised access to your computer systems to steal information and ultimately money from your business.

For example, with malware, if you search for your bank's website instead of typing it in, you might get a pop up asking for login information or a one-time code, giving criminals all the information they need to begin taking money from you. Businesses are reminded to never browse the web for their bank's website, never enter financial information into pop-up windows, and keep anti-virus software up to date.

AIB's Head of Financial Crime, Carol Lawton said "For many businesses Easter is a very busy time for payments, as it's the end of the quarter and also the end of the tax year for many. Criminals will try to take advantage of this period. Fraud can be very distressing for businesses as it often involves significant amounts of money. These scams can be very sophisticated, and criminals go to great lengths to defraud by compromising people's emails or computers, sending emails and messages that appear legitimate, and creating high quality online advertisements, brochures and other materials. We also know that criminals use legitimate names and job titles of people working in various companies, including plausible impersonations, in an attempt to appear genuine.

"AIB urges businesses to be extremely cautious and vigilant at all times. Verify any requests for payments or changes in account details with legitimate, trusted contacts by calling them on known phone numbers; be vigilant against malware that tries to gain access to your systems; always double-check before calling a number provided in an email; check that any website you use is authentic; and remember, if an investment opportunity seems too good to be true, the chances are it is.

At AIB, we are continuously investing to enhance our fraud monitoring systems in response to new and existing fraud trends, and to educate our business customers via online messaging, emails, and targeted social media alerts. We also work closely with industry stakeholders including the Banking and Payments Federation of Ireland (BPFI), and the Gardaí to detect fraud trends, as it's only by communicating and coordinating across the whole of society that we will together be effective."

For more information on AIB's new campaign to help businesses spot the signs and stop fraud before it happens, go to Helping Businesses Prevent Fraud (aib.ie).

ENDS.

Contact louise.y.kelly@aib.ie 087 216 1545