Helping Reduce Scams During Covid-19

Criminals were quick to capitalise on Covid-19. 3% of global spam is estimated to be Covid-19 related, 36% of people in the UK have been contacted by scammers since the start of the pandemic, according to Citizens Advice.

New York City, Jan 7, 2021 (Issuewire.com**)** - Criminals were quick to capitalize on Covid-19. 3% of global spam is estimated to be Covid-19 related, 36% of people in the UK have been contacted by scammers since the start of the pandemic, according to Citizens Advice. Below are some types of fraud to look out for;

Push payment fraud

Push payment fraud is known by a variety of names, including CEO fraud, bogus boss fraud, or business e-mail compromise. It's when criminals impersonate company executives to trick employees into making payments to accounts they control. And it cost UK businesses alone nearly £140 million in 2019, says UK Finance.

Criminals are putting a Covid-19 spin on the fraud by asking businesses to transfer money to accounts supposedly at the Bank of England. We'd advise verifying all requests for transfers, bank or personal details with the organization or individual making the request using established contact details. Do not reply to the e-mail or use the telephone numbers provided — they may be fake.

Consider introducing two-factor authentication for the corporate e-mail system to raise the bar against criminals. And be wary of what you post to social media, company websites, and out-of-the-office messages. It's easy for fraudsters to create a targeted e-mail from such information.

Advance fee fraud

Victims are asked to pay a fee upfront before receiving stock, refunds, rebates, etc. The scammer collects the money and disappears. Covid-19 related advance-fee frauds include selling non-existent medical supplies, landlords purporting to offer retailers a rent deferral in return for a 10% down payment, and fake offers of government assistance, grants, and tax rebates.

Know the habits of your suppliers and business partners. Then you'll stand a better chance of spotting out-of-the-ordinary requests or sudden changes to business practices. If in doubt, double-check with a colleague even when working from home. Check sender e-mail addresses by hovering the mouse cursor over them. Also check they are spelled correctly and come from a corporate account rather than a free e-mail service, such as Gmail or Yahoo.

Tech support, software, and fake anti-virus scams

With more employees now working from home, businesses face a higher risk of being defrauded by phishing and malware attacks. This is when criminals send e-mails that look like they come from trusted sources, such as the IT department.

The e-mails claim that it's time to upgrade the software or anti-virus protection. But really, the criminals want recipients to click on links or open documents that contain viruses or divulge login details or passwords.

Awareness that such scams exist is half the battle. If you're not expecting the e-mail or don't know the sender, delete it without reading. Don't click on links or open attachments. If you're responsible for IT network security, consider e-mail filtering, network segmentation to protect against compromised devices, and strong authentication for more secure areas.

Unusually large orders, new 'customers', fake creditors

We live, work, and trade at unusual times. Nonetheless, be on your guard for new customers placing large repeat orders. Fake creditors are also making the most of Coronavirus cash flow issues. They contact businesses claiming that they are owed money or chasing late payment. They may even threaten legal action, arrest, or removal of goods to cover the value of the debt for good measure.

Criminals are unscrupulous. In uncertain times, they prey on people's emotions, whether that's fear, desperation, generosity, or greed. Being aware of their techniques to guard against them is half the battle in protecting yourself and your business.

Media Contact

Smith Bernards Associates

contact-us@smithbernards.com

Source : Smith & Bernards Associates

See on IssueWire