Stay safe online - blog four - phishing

Blog

20.10.22

Protecting yourself when you go online is a necessity. With a world of information accessible at your fingertips, it is easy to get caught up in the ease of accessibility and on-demand information available. However, you don't want your personal details to be easily accessible for everyone else. Our 'stay safe online' blog series will share tips that you can utilise going forward to protect yourself when interacting with the online world.

Today's blog will cover:

Why is it important to stay safe against phishing or fraudulent schemes?

When engaging online, it is important to be more than just careful - you need to be vigilant. Not everything you read online will be from a reliable source. Phishing scams are used to target

individuals and trick them into providing personal information.

What is phishing?

Phishing is a cybercrime in which fraudulent communications, such as messages or emails, are sent to one or many individuals trying to encourage the recipients to provide sensitive personal data that can then be used to access important accounts or commit identity fraud. The communications appear to be genuine and from a reputable company or a person you trust, for example your bank, your utility provider, a delivery service or even your work colleague. They normally link to a duplicate site that looks legitimate, but when you sign in and enter your details they do not go where you're led to believe, but to a scammer.

How does the scam work?

The individuals behind phishing scams create emails, texts, or web pages that mirror already existing communications or websites from legitimate companies and invite the victim to enter their details, such as passwords for logging in, or card details for making a payment. As the site is fraudulent, any inputted information will go to the scammers.

How can I spot a phishing scam?

A big giveaway would be spelling and grammatical errors. The email address they use could be unusual or different from previous communications from that organisation or person, for example, ending in .com instead of .co.uk or having a completely different domain name.

Other indicators would include offers that seem too good to be true, or create a sense of urgency. An email from a post delivery service stating that you 'missed a delivery' and need to pay a fee to have it redelivered would evoke frustration and urgency which could lead a potential victim to act without thinking. It's important to be mindful of all communications you receive, and to be vigilant about clicking links or entering any sensitive information.

What do I do if I think I've been sent a phishing scam?

First of all, do not click on any of the links, or input any information. If concerned, you can contact the person or organisation that the communication is from - but don't use any of the contact details provided in the potential scam, as they could have that set up to capture more information.

The National Cyber Security Centre outlines what to do if you think you've been sent a scam, and provides advice for reporting a scam email, text, phone call, website, or advert. After you have reported the scam, it is best to delete it from your inbox.

How can I prevent being a victim to a phishing scam?

Avoid putting information online that can be used to identify you. Criminals can use any information available, especially from social media sites, to create convincing communications. For example, one comment on Facebook about who you bank with can then be used to create a spam email 'from' that bank. Although some information sharing may seem harmless, like creating your 'Star Wars name' by putting together the colour of an object on your left and the street you grew up on, any and all information can be used to target you. Be mindful about what you, and others, share about you, and ensure your privacy settings on social media are protecting you.

If you get any communication from TAB that seems strange or out of place please contact us immediately to make sure before entering any personal information.

Stay tuned to read more about staying safe online in this blog series.

This online blog series is an introduction to online safety and designed to raise awareness of the challenges of interacting online. This article is for information only and does not constitute advice or a personal recommendation. When it comes to online activity it is important to be cautious and seek appropriate professional advice.

Capital is at risk. Property values can go down as well as up. Borrowers may default and investments may not perform as expected. Interest and income are not guaranteed. Returns may vary. You should not invest more than you can afford to lose. TAB is not authorised by the Financial Conduct Authority. Investments are not regulated and you will have no access to the Financial Services Compensation Scheme (FSCS) or the Financial Ombudsman Service (FOS). Past performance and forecasts are not reliable indicators of future results and should not be relied on. Forecasts are based on TAB's own internal calculations and opinions and may change. Investments are illiquid. Once invested, you are committed for the full term. Tax treatment depends on individual circumstances and may change.

You are advised to obtain appropriate tax or investment advice where necessary. Understand more about the key risks here.

TAB is a trading name of TAB London Limited. Registered in England and Wales with registration number: 11225821 and whose registered office is at 101 New Cavendish Street, London W1W 6XH.