Online Scams

Shoppers are more easily exploited in the lead up to Christmas, with last minute shopping anxiety making them more susceptible to threats. Online fraudulent activity is becoming increasingly common, with high quality, authentic looking phishing scams being especially difficult to spot.

Amazon customers are the latest victims of an email scam, warns Get Safe Online.

Fraudsters claiming to be from Amazon have sent out thousands of emails to consumers, telling them that there is a 'problem' with their order.

To resolve the alleged issue, the email asks customers to confirm 'certain information' by clicking on a link. Otherwise, they will not be able to access their Amazon account.

This directs people to a seemingly credible but fake website, making it easy for even the most vigilant customer to fall for the scam.

Here, they are required to input in personal information. When customers have entered in their details, they are asked to click a 'Save & Continue' button.

This then takes them to Amazon's official website, again making it difficult for most people to suspect of any fraudulent activity.

Along with being aware of emails asking them to update their details or fix a problem with their account, customers should regularly **check their bank statements**.

Also, looking out for a secure website page is also vital. This can be done by ensuring that the address contains **'https'** at the beginning, with the 's' standing for secure.

A list of basic advice on avoiding these scams have been shared and can be found below:

- Do not click on links in emails, or open attachments in messages from senders you don't know.
- Always use well-known retailers.
- Scammers will often go overboard on requesting more information than necessary to process a payment.
- You should never need to hand over a PIN number to complete a transaction online.
- Browsers and anti-virus protection should be kept up to date regularly to avoid phishing of information.
- The golden rule: If it seems too good to be true - it probably is!

Check out this site

http://www.actionfraud.police.uk/

Paul Hubbard November 2016

Phishing

Phishing can be understood like this: an attempt to acquire personal information via the web for illegal use. In most cases, the fraudsters – purporting to be a reliable, authentic and trustworthy source – are looking for monetary gain. To do this, they need access to data like:

- Usernames and passwords, Bank account details
- PIN number
- Q&A answers (i.e. the answer to 'What is your mother's maiden name?')
- Date of birth, Address

Phishing happens on a daily basis and most of us will usually receive some sort of duplicitous request for information **by email**. Luckily, most of this is automatically spammed, however, every now and again, a sophisticated scam will get through the filters and hit people hard.

Be warned: phishing isn't exclusive to emails. It can come in the form of a seemingly genuine website, social media account and wirelessly (most commonly achieved through **public Wi-Fi).**

What to look out for

Masked in clandestine language, embellished through fancy design and boosted by evoking a sense of emergency – these are all the hallmarks of a typical phishing scam, be it an email, website or social media poll.

At the heart of the attempted fraud is some sort of call to action that encourages you to pass on your personal details. Any seed of doubt that may be planted by an unusual request like this is covered up with clever pretence – they look, act and talk like a professional.

Needless to say, a high quality phishing scam can be hard to spot, which is why so many people end up being conned. However, with vigilance and a cautious attitude, you can shore up your defences. Here are eight key things to look out for:

1. Generic and informal greetings – a lack of personalisation and formality is typical of phishing scams
2. A request for personal information – the core element in any phishing scam
3. Poor grammar – spelling mistakes, typos and unusual phrasing is indicative of a fraud
4. Out of the blue correspondence – unsolicited contact from your bank provider, for example, is highly unusual
5. Unexpected attachments – as with above, if you're not expecting something, think twice before you open
6. A sense of urgency – be wary of statements like "click today" "get in touch asap"
7. Striking gold – if it is too good to be true, then it is too good to be true
8. Peculiar domain names – Why would an English bank send you emails from Peru?

Advice

Don't try and be clever, don't mess about and don't let your guard down. Instead, stick with the most basic and effective solutions at your disposal – ignore, delete, report – and you can be confident you've done well

Paul Hubbard November 2016