

Dangerous email ahead

We've all had them, spam emails pretending to be something they're not, lurking in our inbox waiting for us to get careless and mistakenly click on them before we realize what they are.

Spoof or fraudulent email often pretends to be from a well-known company, such as PayPal, eBay or Sainsbury's, in an attempt to get personal information. People who send spoof emails hope to use your information, such as credit and debit card numbers or account passwords, to commit identity theft.

What can I do to prevent spoofs from affecting me, I hear you mutter? Well, because spoof, or phishing, emails (and the spoof websites often associated with them) are deceptive in appearance it can be all too easy to get sucked in. However, they do contain content that reveals they're fake. The most important thing you can do to protect yourself is to spot this misleading content.

So what should you watch out for?

The sender: Be especially suspicious if it from a sender you don't know. However sometimes your friends can forward spoof emails to you without understanding what they are.

Generic greetings: Many spoof emails begin with a generic greeting, such as: 'Dear member.' Many will simply say 'Hi', 'Hello'

False urgency: Many convey a false sense of urgency and try to deceive you with the threat that your account is in jeopardy if you don't update it ASAP.

Fake links: The text in a link may look valid but on clicking it you'll find yourself sent to a spoof address. Always check where a link is going before you click, by moving your mouse over it and looking at the URL (the web address) in your browser or email status bar. If the link looks suspicious, don't click!

Use of the @ symbol within URLs: Fraudsters will often hide the true location of a link within the URL, but sometimes there will be an @ symbol visible, which will help to pinpoint the actual destination of the link.

Misspellings: Another common technique used is a URL that at first glance is the name of a well-known company but on closer inspection turns out to be slightly altered. For example, www.microsoft.com appears instead as www.micosoft.com. Legitimate companies will not ask certain questions in an email. In fact they should never ask for any of the following information in emails:

- Credit/debit card and bank account numbers;
- Driver's licence details;
- Email addresses;
- Passwords;
- Your full name.

How to prevent spoof emails from affecting you:

- ⇒ Keep your security software current I'm sure you all have anti-virus software installed and many products also come with anti-spam and anti-phishing

components.

- ⇒ Check your bank account periodically to see if there is any suspicious activity.
- ⇒ Change your password if you think your security may have been breached
- ⇒ Use a strong password. A good password contains letters and numbers.
- ⇒ Report fraudulent emails. Forward the entire email, including the header information, or the site's URL, to the company involved immediately. Therefore, if you received a scam email about eBay, you should forward it to them.

Finally, scammers will always play on their victim's paranoia or greed so remember, if something appears too good to be true, it probably is!

Extract from an article by The British Computer Society.