Prepare Your Business

Phishing

Bedfordshire PREPARED

v1.0

What is Phishing?

Phishing is the attempt to acquire sensitive information (e.g. usernames, passwords and credit card details) or steal money by masquerading as a trustworthy entity in an electronic communication such as email, pop-up message, phone call or text message. Cybercriminals often use social engineering techniques to trick the recipient into handing over their personal information, transfer money or even download malicious software onto their device. Although some phishing scams can be poorly designed and are clearly fake, more determined criminals employ various techniques to make them appear as genuine. These techniques can include:

- Identifying the most effective phishing 'hooks' to get the highest click-through rate
- Including genuine logos and other identifying information of legitimate organisations in the message
- Providing a mixture of legitimate and malicious hyperlinks to websites in the message – e.g. including authentic links to privacy policy and terms of service information of a genuine organisation. These authentic links are mixed in with links to a fake phishing website in order to make the spoof site appear more realistic
- Spoofing the URL links of genuine websites – The most common tricks are the use of sub domains and misspelled URLs as well as hiding malicious URLs under what appears to be a link to genuine website which can be easily revealed upon hovering the mouse over it. More sophisticated techniques rely on homograph spoofing which allows for URLs created using different logical characters to read exactly like a trusted domain. Some phishing scams use JavaScript to place a picture of a legitimate URL over a browser's address bar. The URL revealed by hovering over an embedded link can also be changed by using JavaScript

Recent spoofing includes

HMRC, Banks of all types, PayPal, EBay, Amazon, It companies, Lottery, mobile companies, government organisations & DWP, job offers, student loans, BT, talk talk, Virgin media, Apple, Morrison's, Microsoft [plus many others]

Involving

Offers of vouchers, prizes, claiming security issues, direct debit failures and alleged purchase.

Advice

- Do not click those links, to any unsolicited emails
- Contact the companies via their normal websites; inform them of the email and contents
- Do not forward the email, simply snip the email including the header and forward to the company phishing email