purplephish

COVID-19 Phishing Bulletin

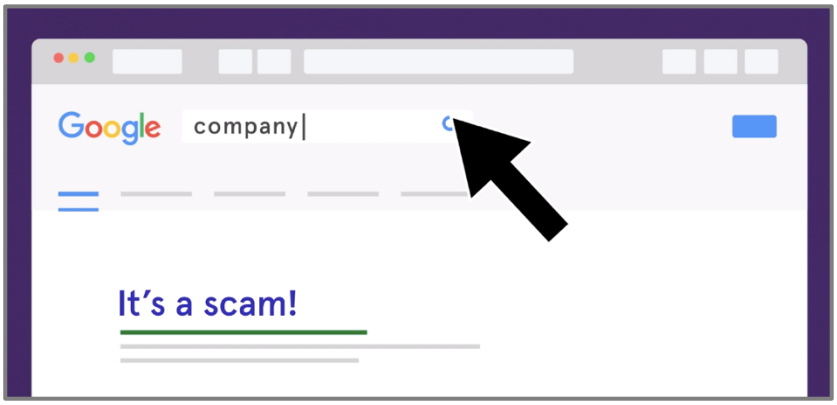
Cyber criminals have long taken advantage of current affairs to make their scams even more convincing: the outbreak of COVID-19 or coronavirus has, sadly, been no exception. In recent days, the National Cyber Security Centre (NCSC) have issued warnings of a sharp uptick in COVID-19 related attacks, with the National Fraud Intelligence Bureau pointing to a 400% increase in coronavirus-themed cyber fraud.

The majority of cyber attacks are using phishing to target employees and gain access to an organisation's data and systems. COVID-19 phishing is commonly imitating organisations involved in healthcare like the World Health Organisation (WHO), the NHS and the US Center for Disease Control (CDC), as well as national governments. The BBC have produced a summary of the most common attacks: https://www.bbc.co.uk/news/technology-51838468.

To feel confident that any email you've received is genuine, you should use the SCAM method.

Sender

- Check the address bar of the email: who is the sender and what is their email address?
- Does the part of the email after the @ symbol match the real website for the organisation the email claims to have come from?
    - If you aren't sure of the organisation's genuine website address, try Googling them and checking the results and also the address bar of their real web page:



- To be extra safe, also hit the email's 'Reply' button. Is the address that appears automatically in the 'To' bar what you would expect?

purplephish

Contents

- Scammers will attempt to imitate the contents and styling of genuine emails and websites closely.
- Just because an email or website includes the logo or uses the corporate colours for a particular organisation or industry body, it doesn't mean that it is genuine.
- Poor use of spelling or grammar is always a very good reason to treat an email or website with suspicion.

Address

- Always be especially vigilant about the web address that any links in an email are sending you to.
- Hover over links with your cursor before you click and check the address that appears. Does it match with the web address for the organisation that the email claims to come from?

- If the web address matches up and you feel confident about clicking, check the address bar once the page has loaded up: did you get taken to where you'd expect? If not, close your browser immediately and report to your IT team.

Mistrust

- Finally, always stop and think: does everything feel right?
- Consider carefully what the email is asking you to do: is it requesting any downloads or for you to enter any personal information or login credentials?
    - Is there any good reason why the sender organisation would require you to do this?
- You should also consider whether an email is expected: can the email's claims or requests be checked by doing a quick Google search?

Remember to use SCAM in its entirety. Cyber criminals are increasingly sophisticated, so just relying on one or two of these tips could mean you fall into their trap.