IN THE SPOTLIGHT
PHISHING ATTACKS

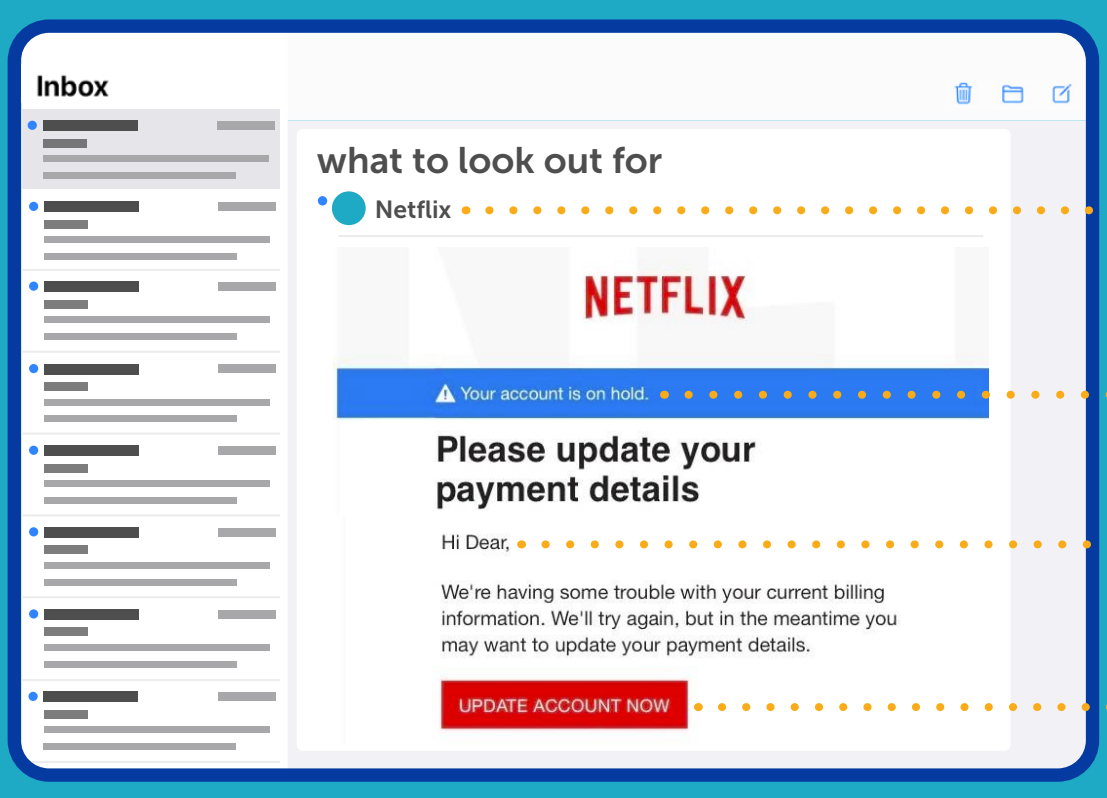
phishing
[fish-ing] *noun.*

The practice of using fraudulent emails to extract sensitive data from users for purposes of identity theft.

Did you know?

82s
is all it takes for someone to fall victim of the attack.

23%
of all recipients of the attack will open the email.



how to spot phishing

Unexpected Correspondance
You don't usually receive emails from them

A sense of urgency exists
They make it seem urgent

Poor spelling, grammar or tone
You aren't referred to by name

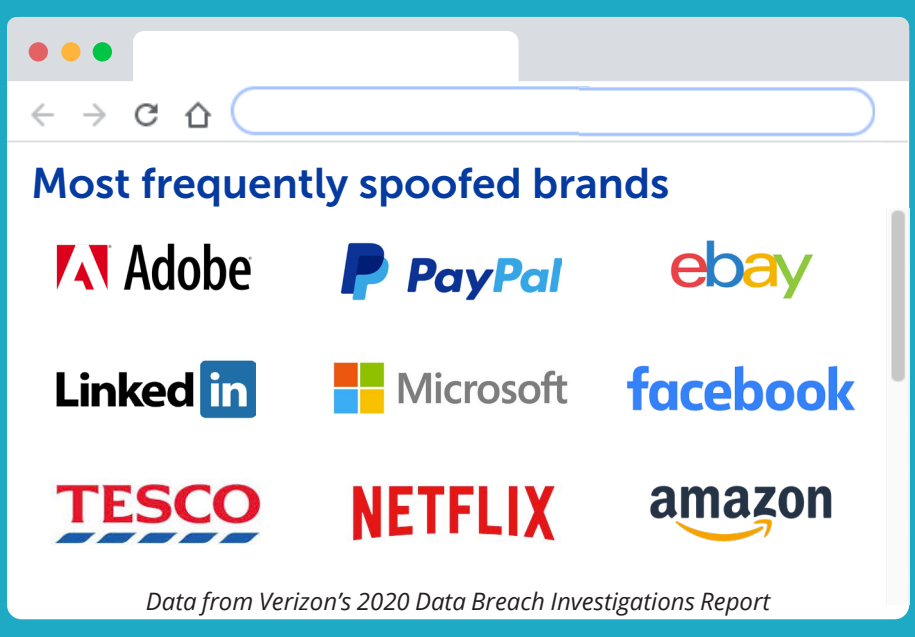
Mismatched URL
Hovering over a button reveals a mismatched link

types of attacks

Phishing attacks can take many forms, but most often they will either be sent as an email attack or as a fake login page.

Attacks can either be wide-spread in nature, such as **email phishing** attacks or highly targeted, often referred to as **spear fishing**.

Personal and professional email accounts can often the target of wide-spread accounts, whereas spear fishing often attacks organisations or high level team members (**whaling**).



Data from Verizon's 2020 Data Breach Investigations Report

what's the difference?
phishing vs spoofing

phishing is used to describe the attack which urges victims to share private details. Phishing often involves spoofing.

spoofing involves attackers mimicking reputable brands, trusted individuals or even clients. Spoofing is the tactic to enable phishing.

how to recognise an attack

Some helpful warning signs to look out for...

do you RECOGNISE the sender?
If you aren't a customer, or don't recognise the sender, chances are it is fake.

is this their REGULAR style of communication?
If you are a customer, but they typically call you for important things, or the way they structure sentences in the email is unusual, this could a sign of an attack.

do links and graphics look AUTHENTIC ?
If the email has images which are stretched, fonts that don't match or links that vary slightly from the typical URL, this is a tell tale warning sign.

is the sender creating URGENCY?
If the sender threatens a negative outcome and urges you to act now, proceed with caution.

how much attacks cost

$500,000,000,000
is the estimated cost of cyber-crime to the global community.

$3,800,000
is the average cost to a company due to a data breach.

Estimates in USD.

how to protect yourself

Cyber security is only as strong as its weakest link, and a lack of knowledge and understanding can put users at risk. Stay safe with these simple prevention methods:

1. Invest in security software
2. Update software and devices regularly
3. Always enable two-factor authentication
4. Back-up data regularly
5. Educate and ask for help

reporting an attack

To:

For Fitz clients, contact us at
020 3727 6020

If you are in the UK, and want to report a suspicious email, forward it to the NSCS at:
report@phishing.gov.uk

If you believe you have fallen victim to an attack, contact Action Fraud at:
actionfraud.police.uk

or you can call them at
0300 123 2020

YOUR PARTNERS IN I.T.

ISO 9001 REGISTERED · ISO 14001 REGISTERED · ISO 27001 REGISTERED · INVESTORS IN PEOPLE | Gold · Gold Microsoft Partner · fitzrovia IT Together