# Phishing

## THE SIMPLE TRICKS HACKERS USE TO STEAL INFORMATION


Phishing is the practice of sending emails pretending to be from reputable companies or contacts, to retrieve your personal information, anything from social media credentials to bank account numbers

The nature of the messages are urgency, threat, terror, greed.

Graphics, logos, sender's name and web links mimic those of real companies.

Remember, if it sounds too good to be true, it probably is!

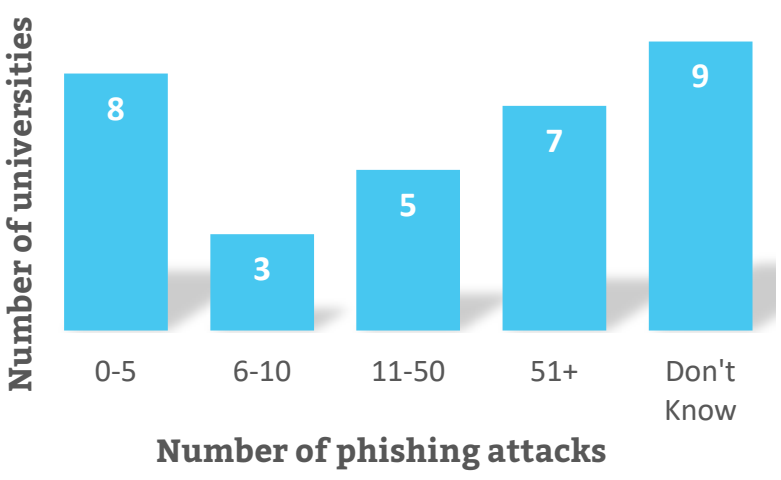
## U.K. universities are not immune to phishing

**70%** of universities have fallen victim to a phishing attack*

7 out of 32 universities have experienced 51+ attacks (2016*)

*"Has your university experienced a phishing attack ?"**

**Yes: 72%**
**Don't Know: 4%**
**No Answer: 24%**




## Types of phishing attack

**Spear phishing** — Targeting specific team, department or individual.

**Smishing** — Scam using SMS/Text messages rather than email.

**Vishing** — Voicemail message instructing you to browse to a malicious web link.

**Clone phishing** — Cloning emails you have previously received from a legitimate company.

**Whaling** — Email targeting executives, department heads or managers.

## Awareness is one of the best defences against phishing!

Look out for
- Attachments
- Links
- Login Buttons

Inspect the body of the email message which contains web links or submit/login buttons.

***WHAT NOT TO DO*** — Reply to the message, click on web links, download attachments.

***WHAT TO DO*** — Report suspected phishing scams to IT Service Desk .

*Source
Article title: Phishing Across the Pond: 70% of U.K. Universities Impacted Website title: The Duo Security Bulletin .URL: https://duo.com/blog/phishing-across-the-pond-70-percent-of-uk-universities-impacted