

Phishing and spam

2010/11 edition

What is phishing?

Phishing is the name given to fake emails that claim to come from organisations like your bank, eBay, PayPal, or even the University. These ask for information such as usernames, passwords and PINs (Personal Identification Number). Phishing is a common form of identity theft.

Note: The University never asks for this sort of information by email. Banks and other financial bodies will not ask for your passwords by emails.

What do phishing emails look like?

The phishing emails will often look just like genuine messages. They may even use colours and logos similar to those used by official organisations.

What would phishers use my details for?

Phishers ask you for information which they then use to steal money from your accounts, buy goods or services in your name or misuse your email account for sending further spam or phishing messages.

What is the difference between spam and phishing?

Spam is the name given to unwanted email sent to your email account advertising goods and services that you have not requested. Phishing email is sent to get information from you, which is then used without your knowledge or permission.

What is the University doing to protect me from spammers and phishers?

The University has introduced a service that filters out spam, suspected viruses and greatly reduces the threat of phishing attacks. The **MySpam** service works automatically and all your emails will be filtered before they arrive in your inbox. If there are any suspicious messages, you will be notified by an email from **MySpam**.

For more details on the MySpam service visit:

www.nottingham.ac.uk/is/computer/email/myspam.aspx



Phishing and spam

2010/11 edition

What should I do if I think I have been sent a suspicious email?

The **MySpam** service should catch most suspicious emails, but if you suspect that you have received a phishing message, you should:

- never reply
- contact the IT helpline on 0115 95 **16677** or email: **student-it-helpline@nottingham.ac.uk**

When/how would the University ask for my username and/or password?

The University never asks for this sort of information by email.

What happens if my email account is disabled by Information Services (IS) because I have been a victim of phishing emails?

In the rare event that IS disables your account, you should contact the IT Helpline on 0115 95 **16677** or email **student-it-helpline@nottingham.ac.uk** to resolve any security issues and to reactivate your email account.

What if I have given my username/password in response to a phishing email?

You should:

- change your password at once
- contact the IT helpline on 0115 95 **16677** or email: **student-it-helpline@nottingham.ac.uk**

How do I change my password?

You can change your password by visiting: password.nottingham.ac.uk and following the online instructions.

