Phishing email scams: protect yourself and your PC
IT Services Documentation Team, March 2014

IT Services will NEVER ask you for your University username/password combination by email. If you receive an email that asks for this information – even if it appears to have come from IT Services or from the IT Service Desk – delete it.

See the reverse of this fact sheet for our quick tips on how to spot a phishing email. You may want to print this out and keep it to hand as a ready reference.

What is phishing?
Phishing is a form of identity theft. Hackers, exploiting our natural human tendency to trust, use spoof emails and/or fake websites to trick us into divulging personal data or downloading malware. It’s a low-tech kind of intrusion that relies heavily on human interaction.

A phishing email may appear to come from a trusted source (e.g. the University, or your bank) and may ask you to provide personal confidential information (password, PIN number, or card details) or to click on a link.

Often the email will have a sense of urgency to it; it may suggest that your bank account is about to be closed, or that your mailbox is over quota. It may even hint at the potential repercussions if you don’t respond.

It may invite you to click on a link within the message or to open an attachment. Doing either could launch executable files or install malware such as viruses on your computer.

How can I tell if an email is a phish?
While some phishing emails are blatantly fake (have you won the Lottery recently?!), many others are more sophisticated.

If you’re not sure if an email is genuine or not, read the content carefully; there are many clues which if you’re vigilant are easy to spot. For example:

- Don’t click on a web link embedded in a suspicious email, or if the email is from an unknown sender. If in doubt, type the link into a web browser manually (don’t copy and paste).
- Or hover your cursor over an embedded link before you click on it. Most email clients and web browsers will reveal where the link will really take you.

For more quick tips on how to spot a phishing email, see the reverse of this fact sheet.

What should I do if I think I’ve received a phishing email?
Don’t respond. Your computing account and your computer could be compromised and the perpetrator could use the information supplied to commit identity theft.

Trust your instincts. If you think it’s a phishing email, it probably is. Just delete it!

If you’re unsure, or you would like advice, contact the Service Desk – servicedesk@abdn.ac.uk or https://myit.abdn.ac.uk/

Why must I be so vigilant?
The University mail filters scan all incoming messages for phishing and spam email.

Email is given a score based on keywords, patterns and blacklists. Any email with a high score is automatically rejected and never makes it as far as your Inbox. Low scoring email is allowed through, but we add **SPAM** to the Subject field to let you know that we think it may be spam. This allows you to decide what to do with it; after all, one person’s junk could be another person’s legitimate correspondence.

Unfortunately, spam filtering is not an exact science and no filtering system can catch everything. It is not always possible to distinguish between valid and unsolicited mail; sometimes valid emails will be rejected, and sometimes phishing emails make it through.

And we’re constantly playing catch up with hackers and spammers as they continue to devise new ways to outsmart mail filters.

IT Security. We are all responsible.
Attention: Your IT account was compromised!

Dear Customer,

We are contacting You because our IT help desk has identified some unusual activity in your university IT account. To prevent fraudulent activity to your account, you must verify your account immediately. If not, we will lock your account.

It's easy:
1. Click the link below to open a secure window.
2. Log in and verify your account details by following the instructions.

Verify my account

Thank you

IT Help Service

---

Forge sender's address

A phishing email may appear to come from a trusted source but it's easy for phishers to forge an email address. To prevent fraudulent activity to your account, you must verify your account immediately. If not, we will lock your account.

---

Fake URL

Sometimes the action of clicking a link can be enough to install malware on your computer, steal personal information, or open you up to social engineering. To persuade you to visit a fake website, emulators may be used incorrectly.

---

Invitation to click on a link

To make you respond without thinking.

---

Impersonal greeting

A generic salutation such as 'Dear Customer' or 'Dear User' can indicate that an email is spam.

---

Spelling mistakes and grammatical errors

Phishers are not known for their spelling and grammar! In addition, misspellings make it easier for messages to bypass 'spam filters'.

---

Alarmist or deceptive subject line

To persuade you to open the email.

---

Sense of urgency and threat of repercussion

To make you respond without thinking.

---

Hover your cursor over a link to see Fake URL.

---

Logo or other branding

To fool you into believing the email is genuine. The image may be of poor quality or be used incorrectly.

---

Alerts or deceptive subject line

A real address. Don't be fooled just because it looks like a trusted source.

---

Invitation to open the email

To persuade you to open the email.

---

Invitation to verify information

To persuade you to verify your account.

---

Still not sure if an email is genuine? Don't click on any links, open attachments, or respond in any way.

---

How to spot a phishing email

Here are some clues that might help you spot a phishing email.

---

IT Services will NEVER ask you for your username/password combination by email.

---

Connect the Service Desk for advice - servicedesk@abdn.ac.uk.

---

Avoid clicking on links in the email.

---

Check that the URL is genuine. Don't click on any links, open attachments, or respond in any way.

---

And remember - IT Services will NEVER ask you for your username/password combination by email.