How to spot a phishing email

Email phishing scams – don’t get hooked!

What’s the easiest way to steal someone’s car? Ask them for their car keys, of course.

That’s how some criminals get hold of your information – they just ask you for it. But, if you received an email from a hacker asking for your username and password, naturally you’d refuse.

Instead, criminals use a technique called phishing to trick you into handing over personal information, usually through email. They then use this information to steal your identity or your money.

Phishing emails are designed to look like they are genuine messages from a company, organisation or someone you trust, for example the University or your bank. They may also appear to come from a legitimate email address or someone in your address book.

A phishing email might ask you to:

- reply directly to an email
- open an attachment
- click a link to a website and fill out a form
- make a phone call

What to look out for

Including some real life examples of phishing emails our staff and students have received.

1. **Does it use your full name?** Phishing emails typically use terms like ‘Dear Customer’ as they do not have your personal details. However more sophisticated scams may use your real name.

   Dear Student,
   
   You have been awarded a University Grant by the Department for Education in the amount of GBP 1829.00. The grant is a one-off grant awarded to students based on a number of criteria which include moral support.
   
   You need to submit your information to collect your grant now. Please click the link below to receive your grant.

   Grant Collection Page
   
   Finance Department
   
   University of Essex

   Here the recipient is referred to as 'Dear Student'.

2. **Suspicious website addresses.** Phishers often mask links to make them appear genuine. If you’re asked to click a link to a website, hover your mouse over the link to see where it’s really pointing to. If the tooltip doesn’t match the link in the email text, don’t click it.
3. **Urgent warnings.** Phishers will try to make you panic. Messages like “if you don’t respond within 48 hours, your account will be closed” convey a sense of urgency so that you’ll respond immediately without thinking.

 Fake warnings about exceeding your mailbox storage quota is a popular method.
4. **Sloppy spelling or grammar.** Look out for Americanisms or strange terminology. Genuine emails won’t be littered with poor grammar and spelling mistakes.

5. **Attachments you aren’t expecting.** Some phishing emails may ask you to open an attachment, for example an order receipt or invoice. These attachments may contain harmful viruses or malware that steal information from your computer.

6. **Different reply-to addresses.** If you click reply, is the reply-to email address the same as the sender address? If it doesn’t match, it’s likely to be phishing.

---

### Think you’ve received a phishing email?

Here’s what to do

Stay calm. Don’t reply to it, don’t action it, just delete it. There’s no risk in simply receiving a phishing email. If you would like a second opinion you can contact the IT Helpdesk.

Please forward the phishing email as an attachment to phishing@essex.ac.uk. Here's how:

- In Outlook, select the email (or emails - you can select multiple messages at once) so it’s highlighted.
- Click the *More* button and select *Forward as attachment*.

- In the To field type phishing@essex.ac.uk and then click *Send*. 

---
<table>
<thead>
<tr>
<th>From</th>
<th>To: Team Report</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Co:</td>
</tr>
<tr>
<td></td>
<td>Bcc:</td>
</tr>
<tr>
<td>Subject:</td>
<td>P Warwick Organiser now available</td>
</tr>
<tr>
<td>Attached:</td>
<td>HR Organiser now available (33 KB)</td>
</tr>
</tbody>
</table>