University of Essex

Phishing

What you need to know

What is phishing?

Phishing is the use of fake emails that claim to be from a reputable company, organisation or someone you trust. Their aim is to trick you into handing over personal information, such as your bank details and passwords.

It happened here

September 2017: A University computer was infected with ransomware which encrypted files on network shares.
October 2017: A member of University staff was the victim of a phishing scam which resulted in their salary being paid into the thief's bank account.

What's the worst that could happen?

Identity theft
Thieves can use your identity to commit almost any crime imaginable in your name, such as entering (or leaving) a country illegally, cyber crime and money laundering. You could find yourself part of a criminal investigation.

Financial fraud
Fraudsters could potentially empty your bank account or buy things using your bank details. They can also use your identity to commit other financial frauds and ruin your credit rating.

Fines and reputational damage
The University could be fined for financial irregularities or failing to look after personal data. Major press coverage puts people off applying to study or work with us.

Data and information loss
Ransomware can encrypt your or the University's data, and we may have to pay a ransom to get it back. This stops us accessing information about staff and students.

How to spot a phishing email

1. **Spelling and bad grammar**
Genuine emails won't be littered with poor grammar or spelling mistakes. Also look out for unfamiliar phrases.

2. **Beware of links in emails**
If you're asked to click a link to a website, hover over the link to see where it's really linked to. If the link doesn't look quite right, don't click it.

3. **Threats and urgent warnings**
Phishers often use urgent messages to cause panic so that you'll act immediately without thinking. Take your time to read the email.

4. **Suspicious attachments**
Don't open attachments you aren't expecting, especially from someone you don't know. They may contain harmful viruses.

5. **Does it use your name?**
Phishers often use generic greetings like 'Dear Customer'. However more sophisticated scams may use your real name.

6. **Strange sender or reply address**
If you click reply, is the reply-to email address the same as the sender address? If it doesn't match, it could be phishing.

Phishing is real and **everyone** is a target

Think you've received a phishing email?
Stay calm, don't reply or click any links, just delete it. There's no harm in simply receiving a phishing email. To report a phishing email, forward it to: phishing@essex.ac.uk