



PHISHED

ADAM JENKINS, UNIVERSITY OF EDINBURGH

PhishEd Team: TULiPS Group



ADAM JENKINS (RA)

adam.jenkins@ed.ac.uk

@adamdgjenkins18



NADIN KOKCIYAN (CO-PI)

nadin.kokciyan@ed.ac.uk

@nkokciyan

nadinkokciyan.com



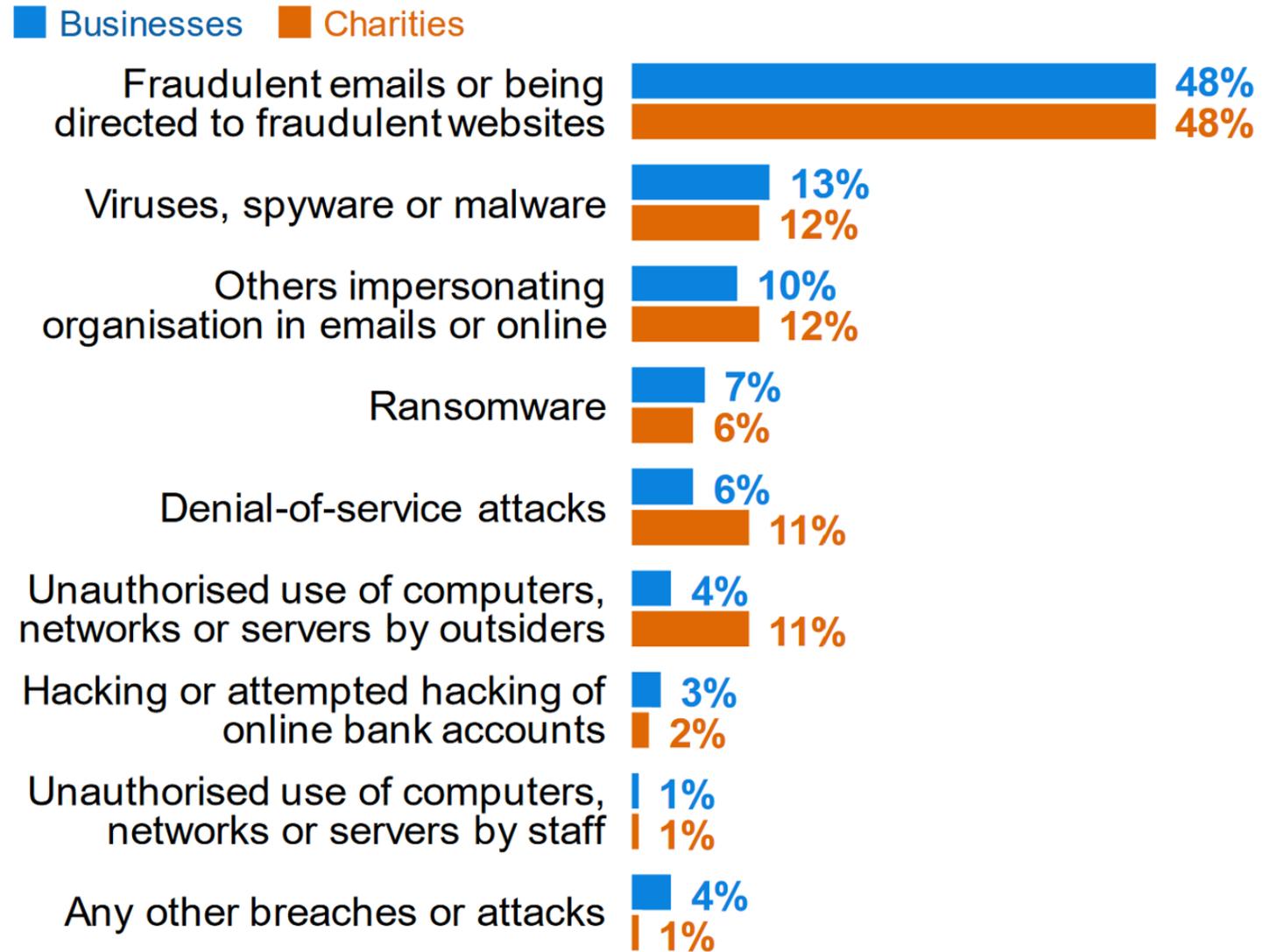
KAMI VANIEA (PI)

kvaniea@inf.ed.ac.uk

@kvaniea

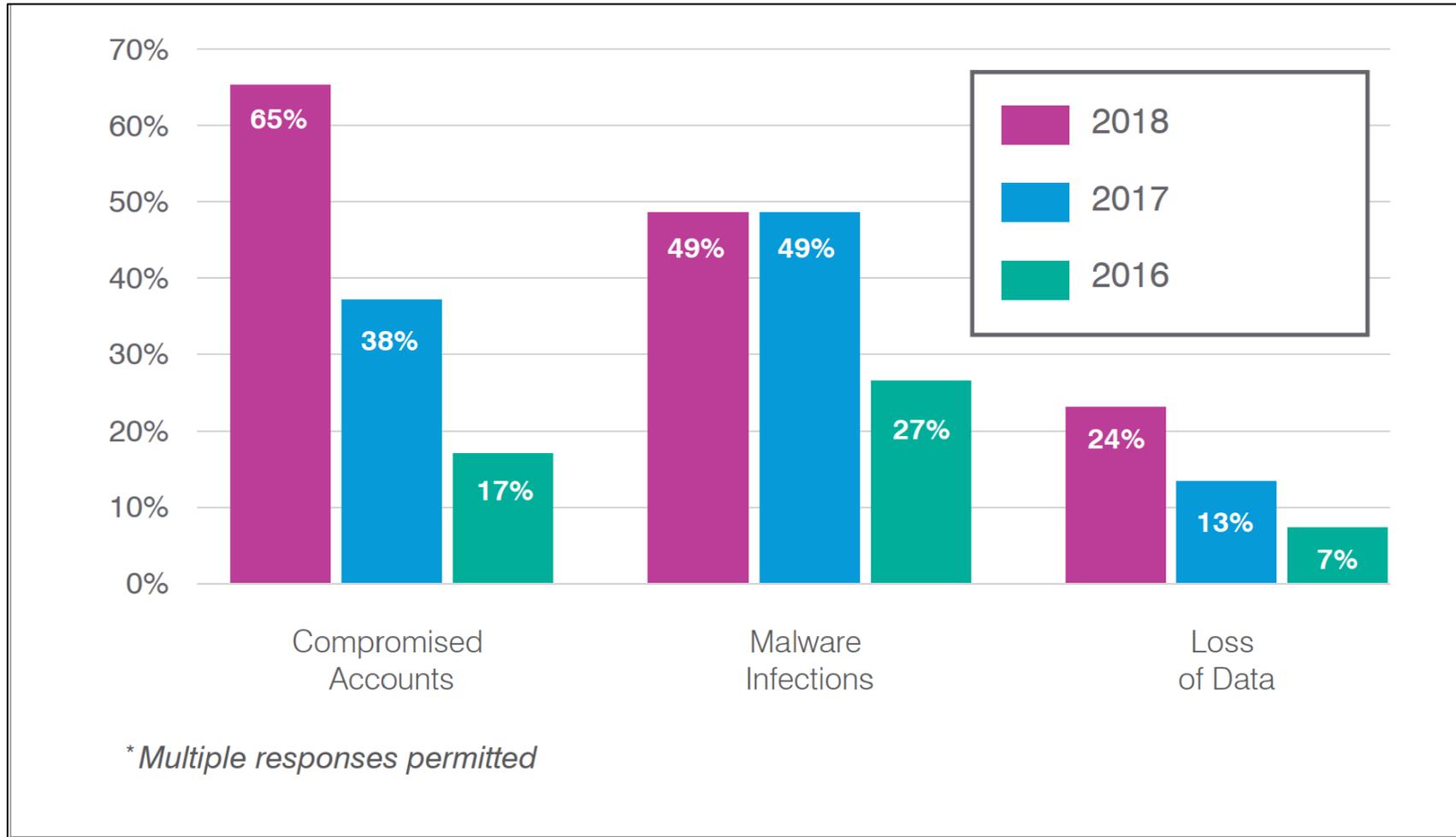
vaniea.com

Phishing is a very common issue faced by UK businesses



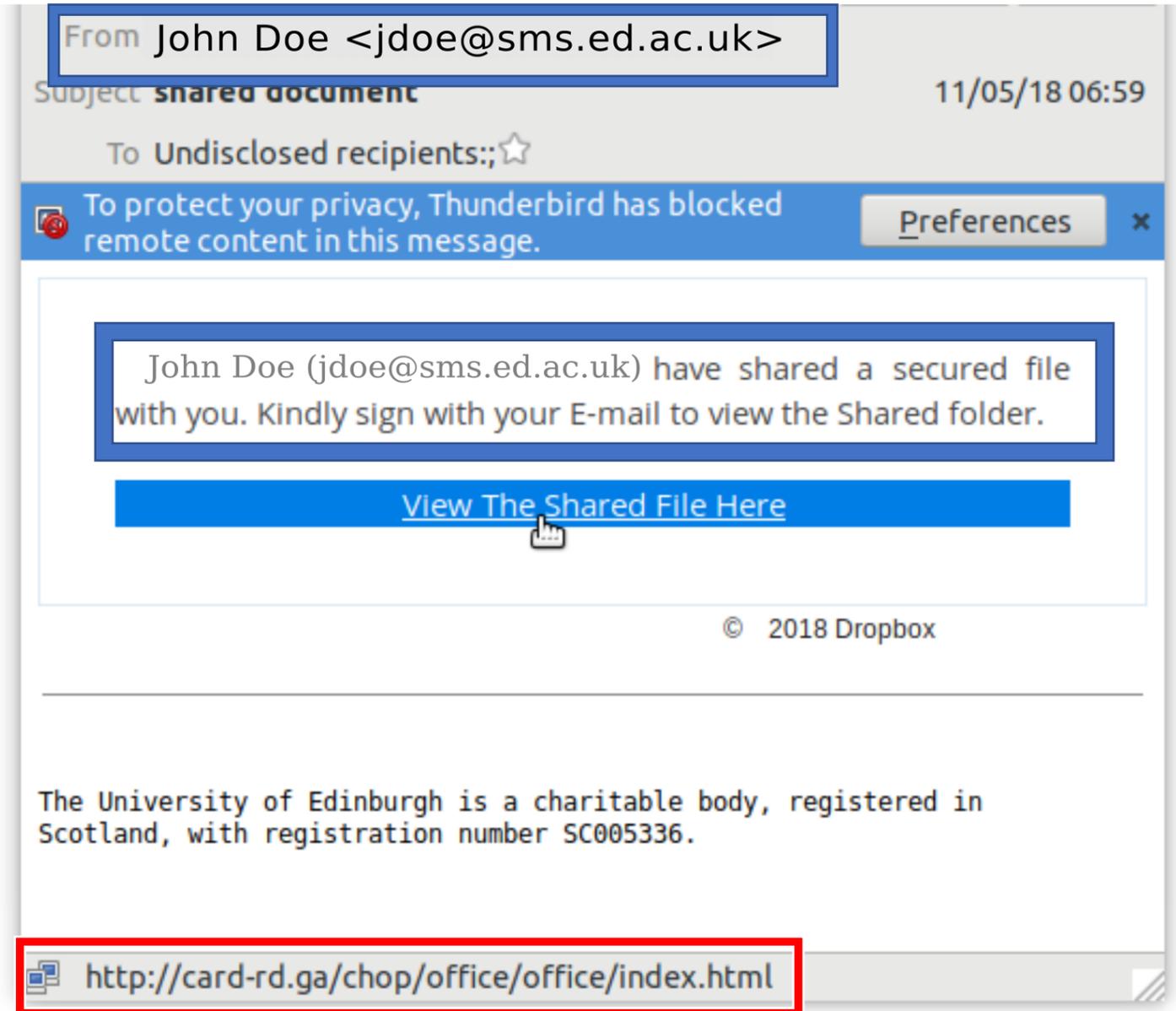
Bases: 778 businesses that identified a breach or attack in the last 12 months; 218 charities

Phishing Impacts



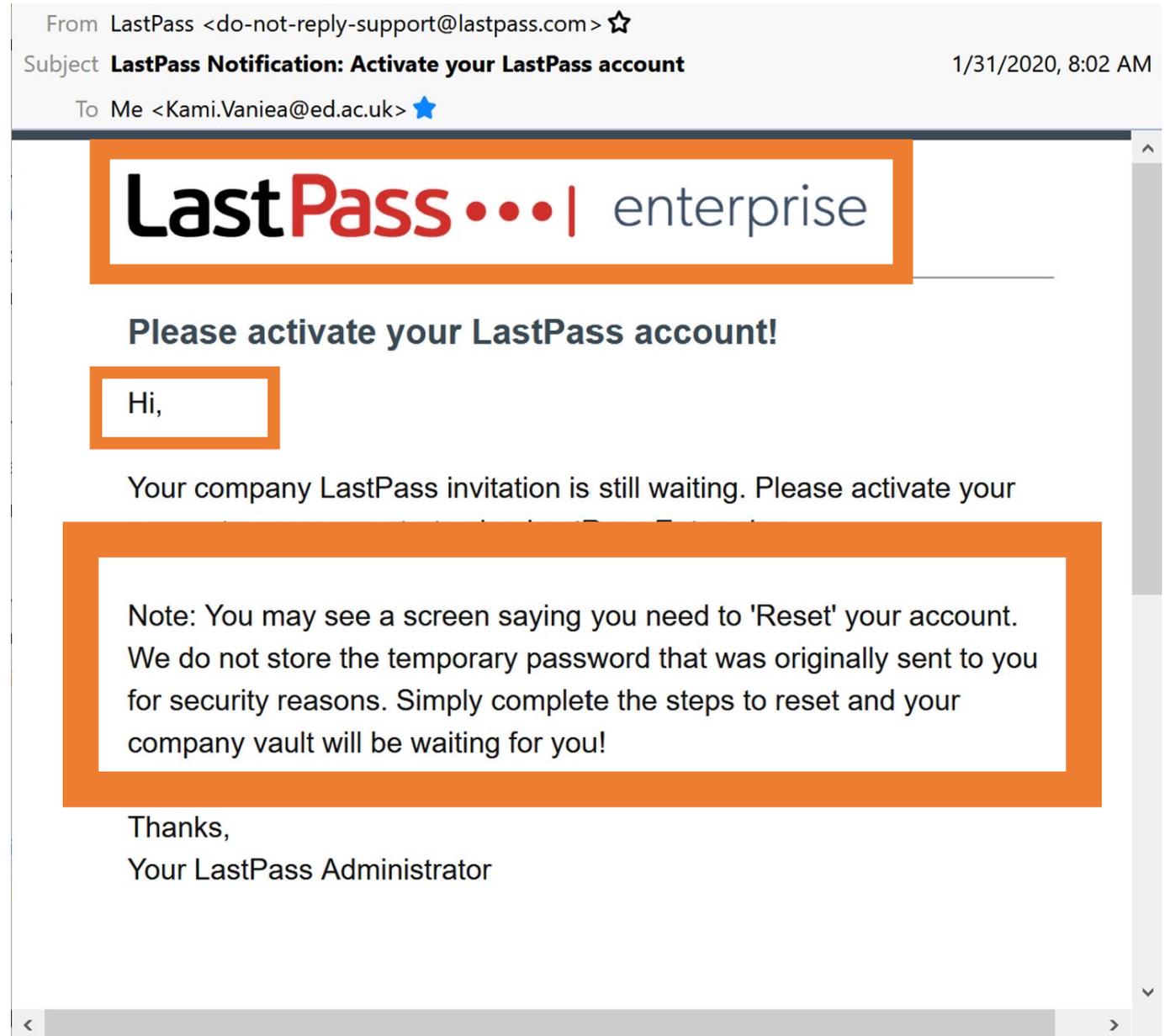
Phishing is hard for Users to detect!

Attackers will use a range of Techniques to 'spoof' emails, looking like genuine emails.

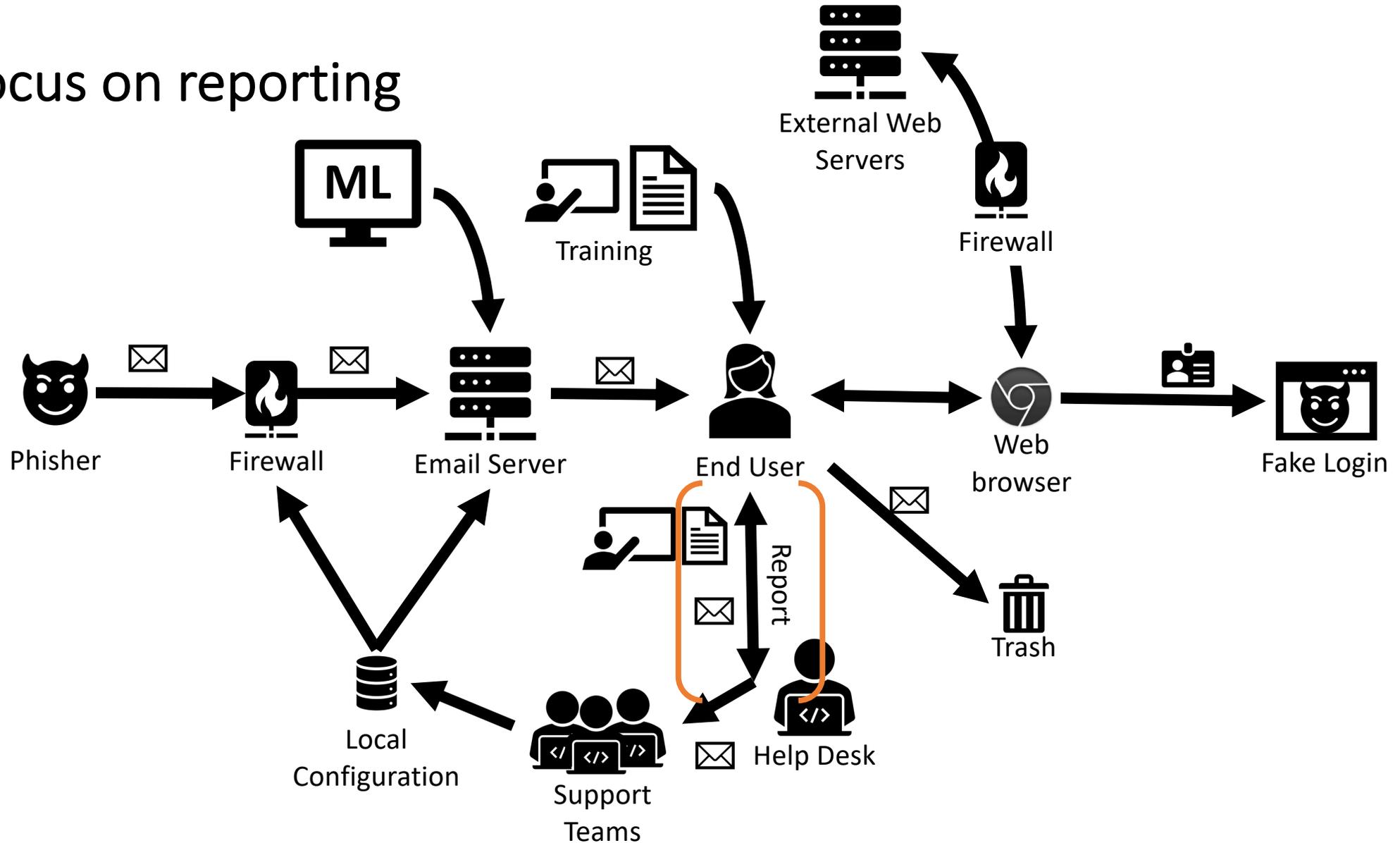


Phishing is hard for Users to detect

Attackers will use a range of Techniques to 'spooF' emails, looking like genuine emails.



We focus on reporting



Hello,

This is an automatic reply to confirm that your message has been received by the Virgin Media Customer Information Security Team. Your report has been assigned the following reference number: 2148293

If you have received an email from us (5th March 2020 or later) about your personal information, you can find out more details at virginmedia.com/data

If you require support regarding a security issue, please visit virginmedia.com/securityhub.

Virgin Media is dedicated to ensuring that its Broadband service is used in a manner that is consistent with its Acceptable Use Policy (AUP), which forbids abusive or offensive conduct, as well as performing network attacks or sending spamemails.

The Internet Security team take all reported abuse complaints seriously, and will handle them in accordance with the above policies. All submissions are investigated thoroughly and the AUP will be enforced if necessary.

If you have reported a security threat or supplied intelligence about a vulnerability/bug on Virgin Media systems or infrastructure, please ensure that you have supplied sufficient contact information and we will be in touch as soon as possible.

This however may be the last reply that you receive unless more information is required.

For more details on reporting abuse from a Virgin Media IP address, including the standard of evidence we require in order to investigate a complaint, please visit virginmedia.com/abuse

Thank you for your report.

Kind regards,

Virgin Media Customer Information Security

From John Doe <jdoe@sms.ed.ac.uk>

Subject **shared document**

11/05/18 06:59

To Undisclosed recipients;;★

To protect your privacy, Thunderbird has blocked remote content in this message.

[Preferences](#) ×

John Doe (jdoe@sms.ed.ac.uk) have shared a secured file with you. Kindly sign with your E-mail to view the Shared folder.

[View The Shared File Here](#)

© 2018 Dropbox

The University of Edinburgh is a charitable body, registered in Scotland, with registration number SC005336.

<http://card-rd.ga/chop/office/office/index.html>

PhishED

PROJECT GOALS



- Design of phishing advice templates
- Provide case studies for template usage based on user reporting behaviors
- Develop Outlook Plugin using Microsoft Graph API

- **Focus groups – Design based**
- **Lab studies**
- **Longitudinal field study**



METHODS

Rede for A Influenc

- Kelley W. (2017) In Proc Privac
- Altho (May). phish Proce Humc 17).
- Zeyu : Phish Unive

 **Thank You, Zeyu!** Your Inquiry ID: 10083

Your report makes you and others safer. And we have checked this email for you.

Take Your Time!
Don't click any links, buttons or attachments yet. They may be used to get your privacy.
Calm down, legitimate organizations usually don't ask you to respond within minutes or hours.

We can't guarantee it is phishing or not, but you can!

Found Danger 2	Sender's From Outside the University	Links Inside 1	Email Language Possible Dangerous
--------------------------	--	--------------------------	---

Fact Clean Possible Danger Dangerous

 **This email is from:**
elxw.fa.sender@workflow.mail.em3.oraclecloud.com

Sender's Domain
oraclecloud.com
This is the sender's email address, which should match the name that they tell you.

Authentication No authentication deployed <small>Nobody authenticates this domain.</small>	Domain Check Domain is not stolen from others <small>This domain is indeed held by the sender.</small>
---	---

Sender is From
Outside the University
Messages related to the University activities should be sent inside.

 **There is 1 link in this email:**
leboncoinpaiementpro.fr

Destination Domain
leboncoinpaiementpro.fr
This is the sender's website address, which should also match the name that they tell you.

Domain Age 1 Month <small>Is it too young for a big organization?</small>	Domain Location Amsterdam, Netherlands <small>It should match where the sender from.</small>
--	---

Search Result
Not matched
We didn't found a popular website by this domain.

 **No other strange things are found in this link.**

 **We have also scanned the languages in this email.**
Be aware of folloing findings.

Recipient Title
Your name is not referred
Legitimate organizations usually refered you by name in important emails.

Phishing Keyword
Access
We have found some words that are frequently included in phishing emails.

You are the most suitable one to judge this email.
If you see many red/yellow ones, be particularly careful.
Only you know what are you expecting or not.

Still confused?
Just email your Inquiry ID to xxx@eee.com, one of our team will get to you within 24 hours.

Your Inquiry ID: 10083

his link.

Domain Popularity
Low

appear in this URL.

ge.ru/...

have.

not popular

not popular

not match your URL:
iot.com/



THANK YOU & QUESTIONS?



ADAM.JENKINS@ED.AC.UK



[HTTPS://GROUPS.INFO.AC.UK/TULIPS/](https://groups.inf.ed.ac.uk/tulips/)