PHISHING ATTACKS: LEARNING BY DOING

Tom Chothia, Stefan Paul and Michael Oultram

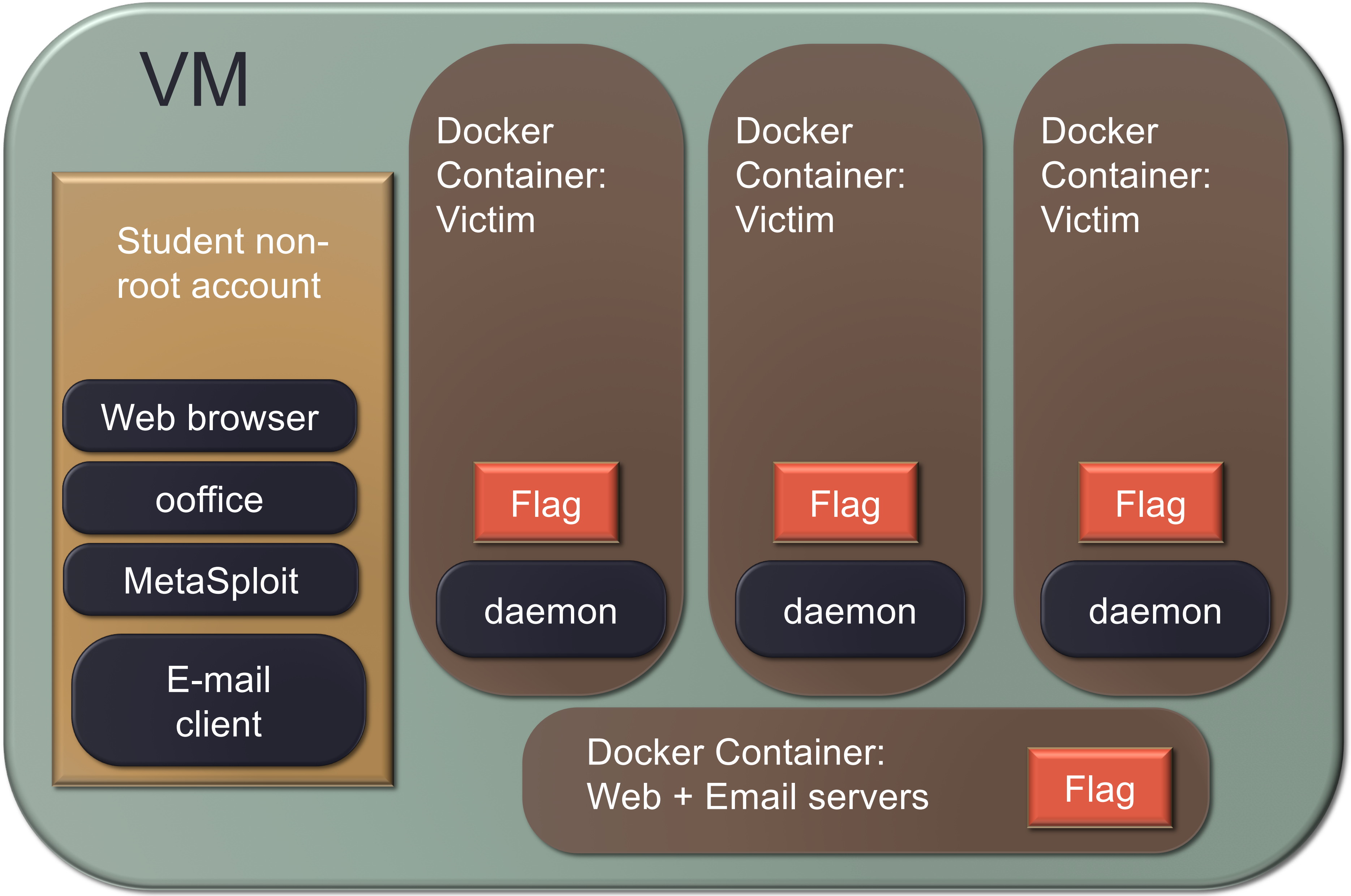
University of Birmingham, UK

Teaching Phishing Attacks is Hard

- “People fall for phishing attacks because they are stupid”
- “I’d never fall for a phishing attack”
- Phishing attacks work because people are not thinking about phishing attacks when they open their e-mail.
- When you teach phishing attacks the students will be thinking about phishing attacks.

Our Solution

- A VM framework in which students can perform their own phishing attacks.
- The VM contains a company website.
  - More information about the employees can be found on Facebook.
- Docker containers, running our scripts simulate each possible phishing victim.
- Students need to think about the employees, look at their profiles, and come up with ideas for spear phishing attacks.
- They must then execute these attacks on the VM using Metaspoit, Office macros, and by building fake websites.



VM

Student non-root account

Web browser

ooffice

MetaSploit

E-mail client

Docker Container: Victim

Flag

daemon

Docker Container: Victim

Flag

daemon

Docker Container: Victim

Flag

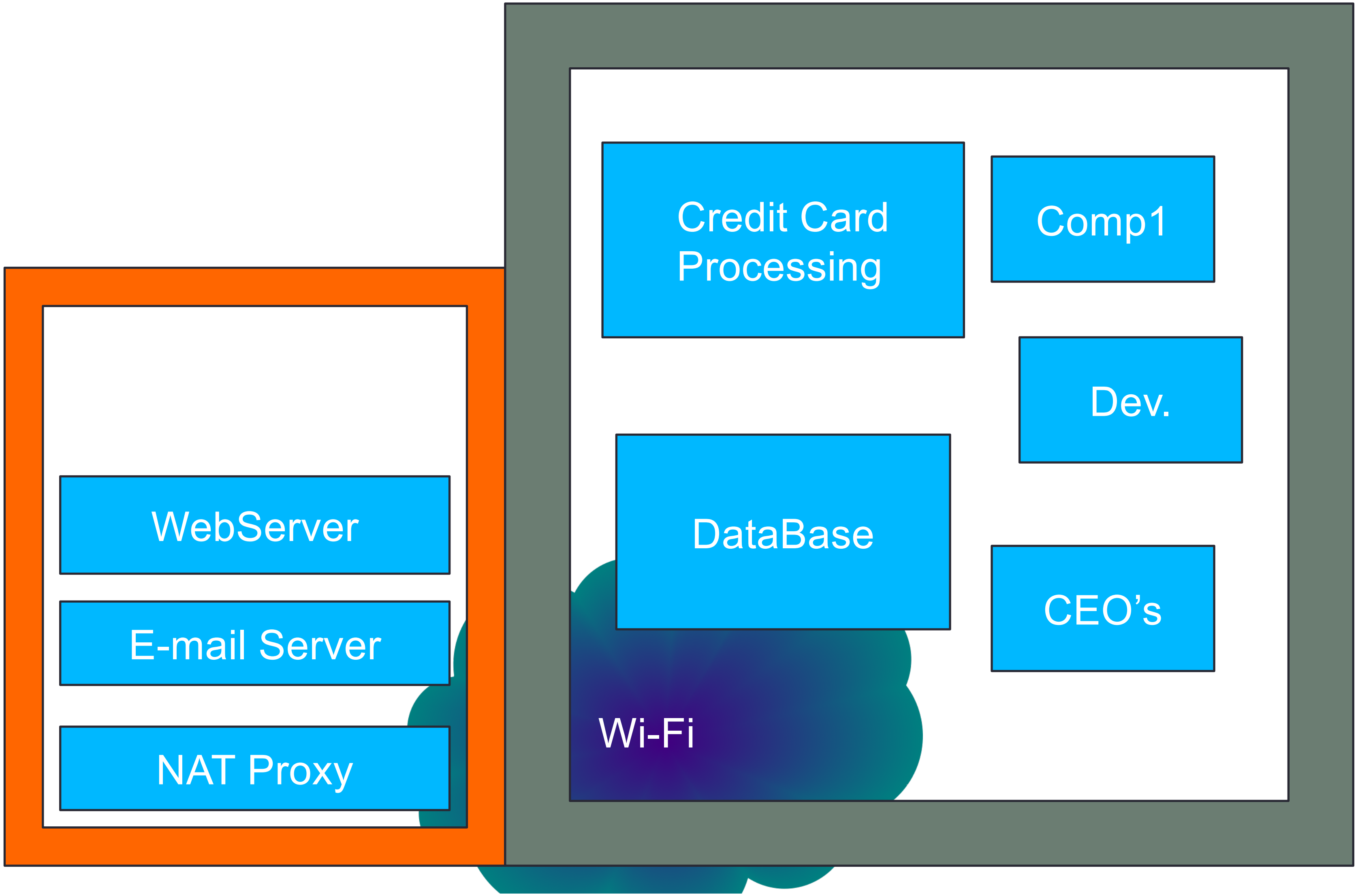
daemon

Docker Container: Web + Email servers

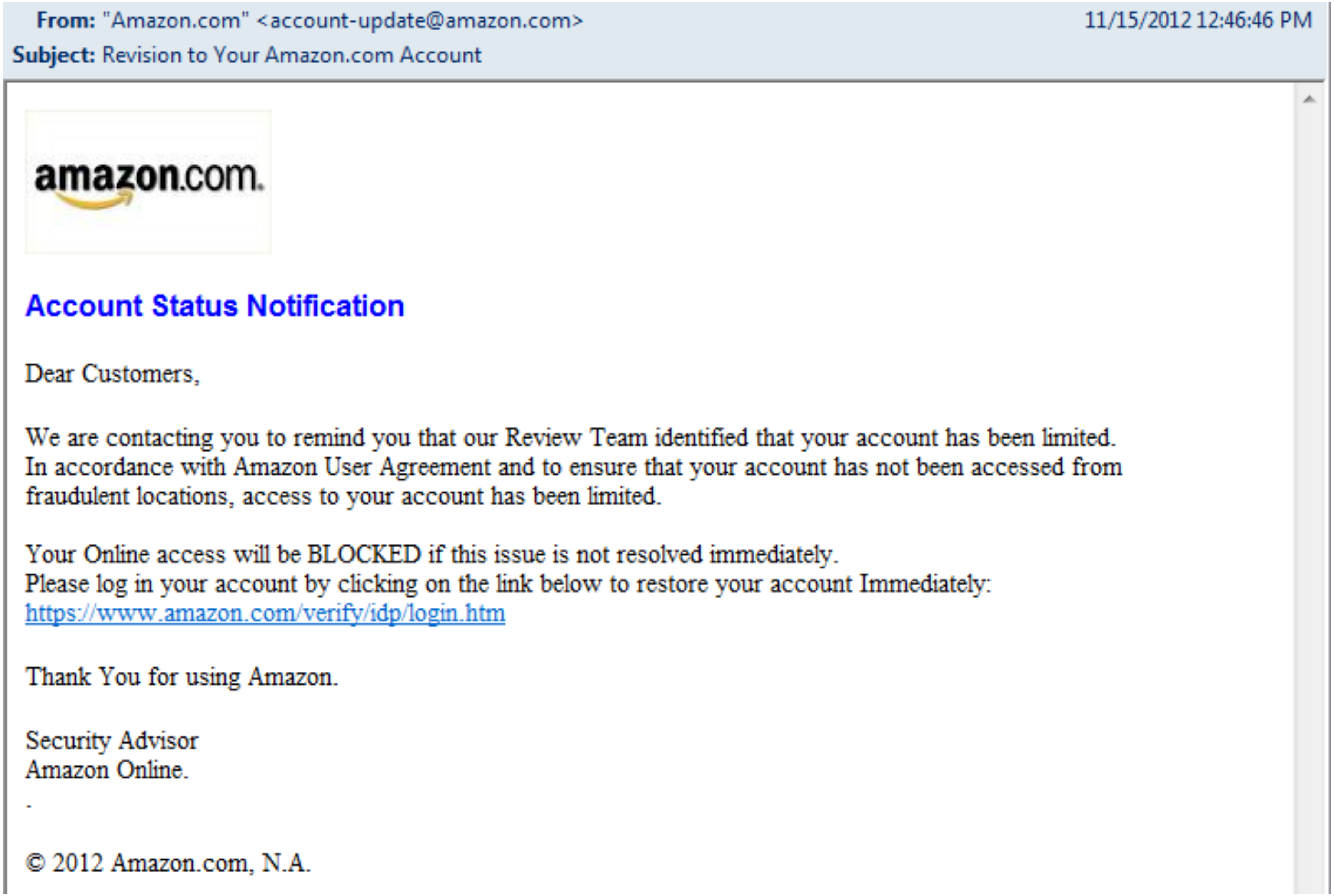
Flag

LESSON OVERVIEW

A Typical Network



Phishing



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM

Subject: Revision to Your Amazon.com Account

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited. In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

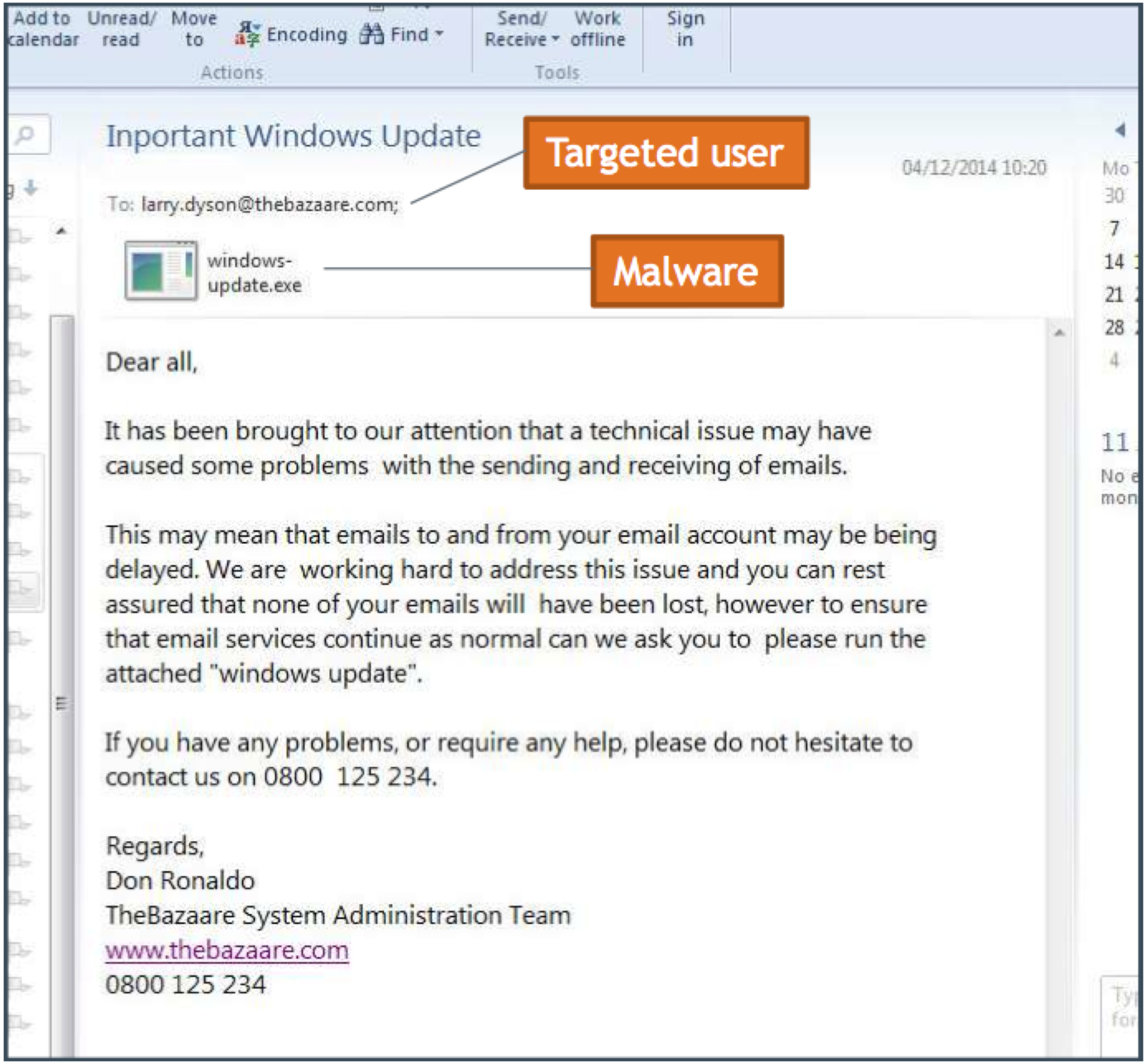
Security Advisor
Amazon Online.

-

© 2012 Amazon.com, N.A.

Spear Phishing

- Random phishing e-mails don’t stand much chance.
- Spear phishing refers to very carefully crafted, targeted phishing e-mails.
- E.g. look on Linkedin, Facebook:
  - find the name of the sysadmin,
  - find the name of a new employee and
  - write an e-mail which makes the new employee fear they are going to loose out.



Inportant Windows Update

04/12/2014 10:20

To: larry.dyson@thebazaare.com;

Dear all,

It has been brought to our attention that a technical issue may have caused some problems with the sending and receiving of emails.

This may mean that emails to and from your email account may be being delayed. We are working hard to address this issue and you can rest assured that none of your emails will have been lost, however to ensure that email services continue as normal can we ask you to please run the attached "windows update".

If you have any problems, or require any help, please do not hesitate to contact us on 0800 125 234.

Regards,
Don Ronaldo
TheBazaare System Administration Team
www.thebazaare.com
0800 125 234

from MWR infosec.

Phishing payloads

- Websites,
  - E.g. phishtank.com

- Executables
  - Run anything you want

- Macros
  - In office documents

But the real question is how to get people to open the payload!

Automated flag submission

- Students can be asked to write up their attacks.
  - Give their reasoning, and say why the victim might fall for the attack.
  - Marks can be awarded for good idea’s that didn’t work.

- Marks can also be just for flag submission
  - Done automatically via a website:
  - http://www.cs.bham.ac.uk/internal/courses/comp-sec/publictokens

Further work

- Improve performance
  - 8GB VM! Some scripts can crash (e.g. on special characters in e-mails)E.g. – restart fixes this.
- A.I. methods to recognize tone and text for e-mail.
- Getting past different levels of anti-virus.
- More sources of information.
- Assessment of educational value.

Please do let me know if you would like to use or help develop this.