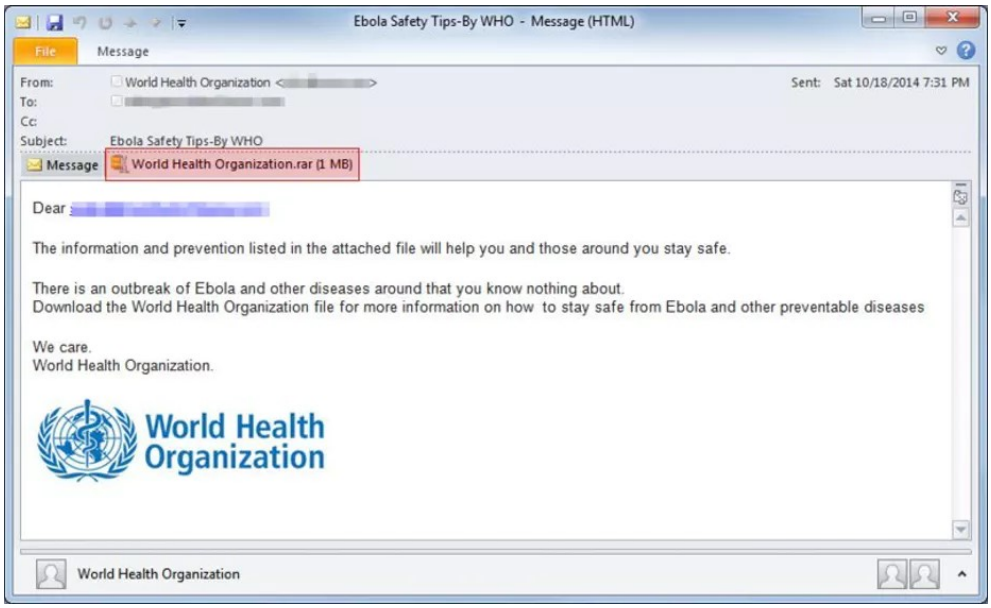
THE CONVERSATION
Academic rigour, journalistic flair

In cybersecurity, the weakest link is … you

October 31, 2014 3.03pm GMT



We should know by now - don't click that link. Bill Buchanan, Author provided

Author

Bill Buchanan

Head, Centre for Distributed Computing, Networks and Security, Edinburgh Napier University

A chain is only as strong as its weakest link. Computer security relies on a great number of links, hardware, software and something else altogether: you. The greatest threat to information security is actually people. Why strive to defeat encrypted passwords stored in computers, when those computers' human users will turn them over willingly?

The technique is known as social engineering. It could be a phone call at your desk "from IT" querying problems with your login details, or asking about those of our colleagues'. Or the more common technique of phishing – emails designed to solicit your credit card or login details by passing themselves off as legitimate emails from well-known banks or websites such as PayPal or eBay. This has evolved in spear phishing, in which known details about you personally gives the email even greater credibility.

The latest ruse are emails purporting to be from the World Health Organisation about Ebola, with email subjects including:

"Ebola Safety Tips - By WHO."

“What You Need To Know About The Deadly Ebola Outbreak,”

“So Really, How Do You Get Ebola?,”

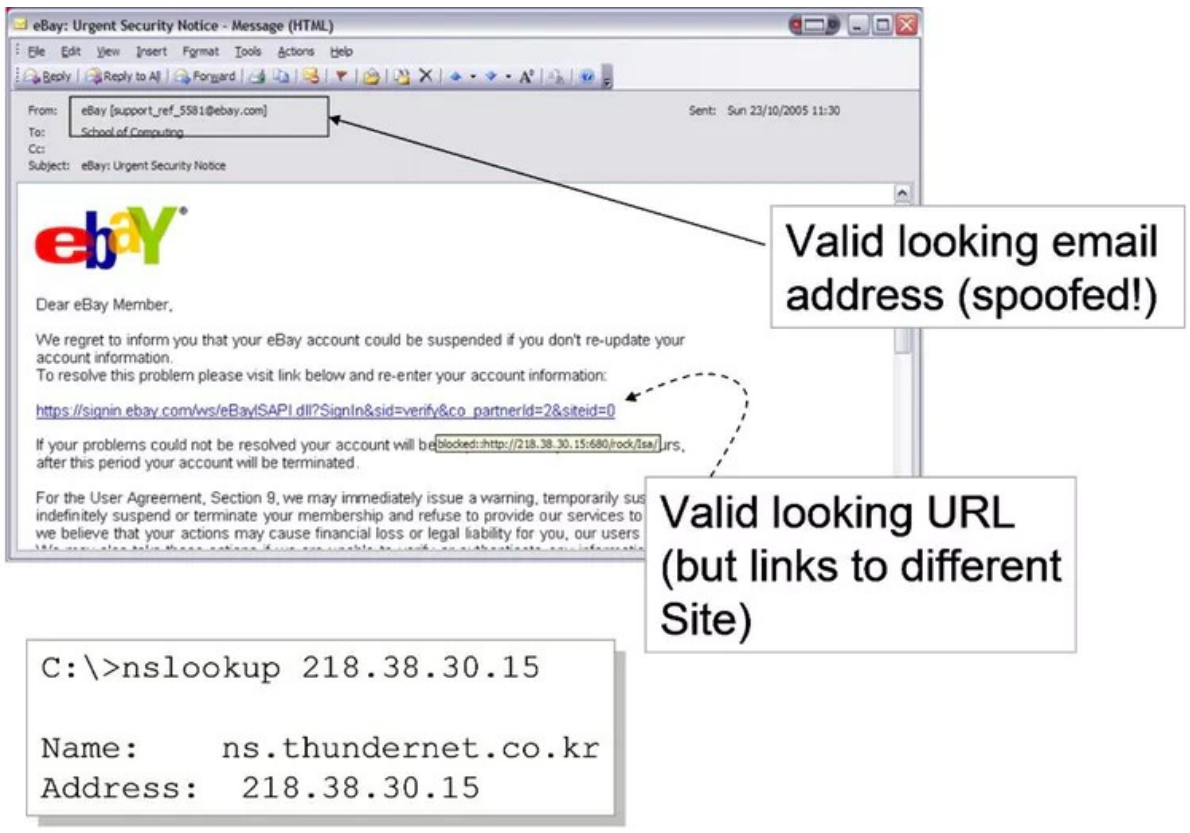
“Is there ANY way to cure Ebola?”

“The #1 Food Items You’ll Need In An EBOLA Crisis.”

But the link to the attached file which is described as health guidelines instead installs the DarkComet Trojan malware that gives attackers remote access to your computer. Any current event is fair game for cybercriminals if it can tempt you to click that link.

Spoofed addresses

A major problem with most types of digital communication, processing and storage is that it’s often difficult to differentiate between a true event or one which has been falsified. This stems largely from the internet’s origins as an open, insecure system. In this email apparently from eBay, the email address of the sender has been spoofed, that is, replaced with another that is not the sender’s actual address, as some email relay systems allow this.



Addresses are not as they seem. Bill Buchanan, Author provided

Take a look at the full email headers, however, and the entire route the mail has taken from source to destination is clear, as is the fact the sender is not verified:

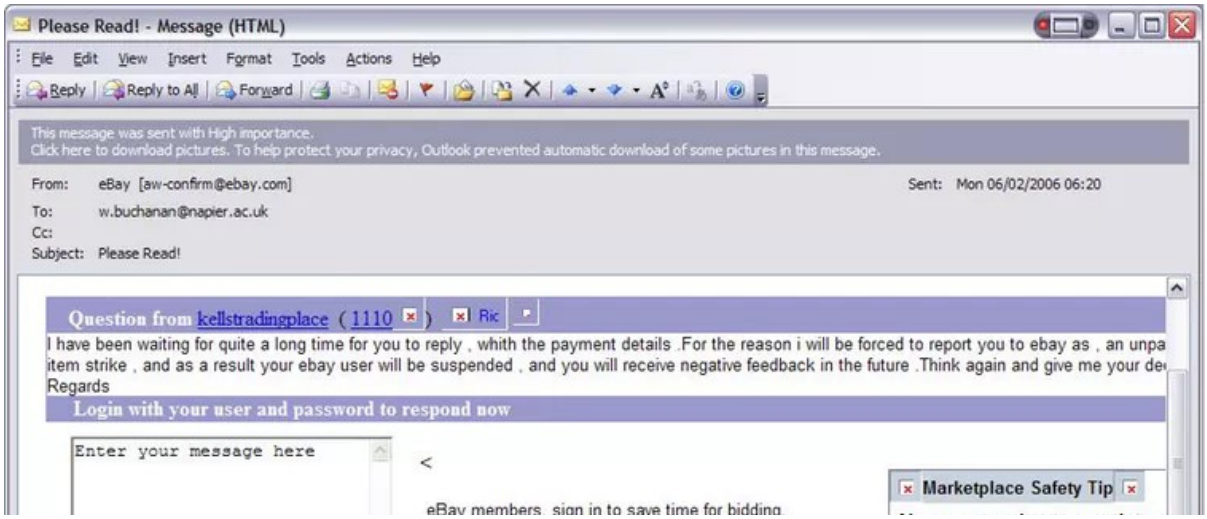
> *Microsoft Mail Internet Headers Version 2.0*
>
> *Received: from mer-w2003-6.napier-mail.napier.ac.uk ([146.176.223.1]) by EVS1.napier-mail.napier.ac.uk with Microsoft SMTPSVC(6.0.3790.1830);*
>
> *Wed, 18 Jan 2006 00:17:45 +0000*
>
> *Received: from pcp0011634462pcs.ivylnd01.pa.comcast.net (Not Verified[68.38.82.127]) by mer-w2003-6.napier-mail.napier.ac.uk with NetIQ MailMarshal (v6,1,3,15)*
>
> *id*
>
> *FCC: mailbox://support_id_1779124147875@ebay.com/Sent*
>
> *Date: Tue, 17 Jan 2006 17:10:39 -0700*
>
> *From: eBay*

And when the user clicks the link they find themselves at a Korean web site, not ebay.com, which requires the user to login with their genuine eBay credentials – essentially handing over their keys.

Spoofed email

Most people will spot this as a fake these days, but if there's additional information that tricks the reader into thinking a human wrote the email, prompting them for interaction, it can generate better results.

> *I have been waiting for quite a long time for you to reply, whith the payments details . For this reason I will be forced to report you to ebay as an upaid item...*



Spoofed emails, with a human touch. Bill Buchanan, Author provided

This pressures the reader – no one wants bad eBay feedback, after all. Looking at the email's HTML reveals the con (if the poor spelling and punctuation typical of such emails wasn't enough) as a hidden form element shows that the user will be taken not to ebay.com but to a server in the Czech Republic (<form method="POST" action="http://www.mailform.cz/en/form.asp">) which, while looking exactly like eBay, will only steal the user's credentials

Sharp spears

Increasingly it is the spear in spear phishing that is being sharpened, with criminals pulling together more details about you to make their efforts to make you open your wallet more convincing. For example, sending a message apparently from the same bank with which you have an account.

It's not just home users under attack – corporates are targeted too, and with the growth in hacking attacks linked to nation states and overseas governments, sophisticated and sustained campaigns of spear phishing have succeeded in stealing information from firms and organisations across Europe. Symantec recorded a 62% rise in data breaches from spear phishing in 2013.

The answer has to be better training and keen user awareness. Because for all the tools included in browsers and email readers to try and help users spot these deceits, many still fall for highly targeted phishing mails – and often only one user with access to a corporate site is required for attackers to ratchet up their access to the network.

As the Institution of Engineering and Technology recently told a parliamentary committee, now that we all use computers, all of the time, security is far too important to leave to just a few specialists.

Online security **Cybersecurity** **Computer hacking** **Cybercrime** **Ebola outbreak** **Phishing**