White Paper: Spam

A dangerous time waster

Introduction

It's estimated that 80% of all email sent in the entire world is spam. Only 2 in 10 emails are legitimate. That's a LOT of spam. And spam isn't new - it's been around since email was invented in the 1980's. While this old enemy may seem easily avoidable for some, it remains the no. 1 cause of viruses entering and infect staff computers or even entire networks. This white paper will explain what to look out for, provide some tips on spotting fake emails – even those that look very real - and how you can reduce your exposure to spam longer term.

Surely no-one believes those fake emails!?

You'd be surprised. Some people do actually believe they can buy cheap medicine online, or have certain parts of their bodies "enhanced", or that they have indeed missed a FedEx delivery they weren't expecting. One survey put it as high as 30% of people opening and reading these emails. The very fact that spam exists means it works, it makes money, and it funds criminals devising ever more sophisticated ways of conning people.

Why can't my anti-spam protection stop them?

The challenge with any type of security protection – anti-virus, anti-spam etc. – is that the attacks are constantly changing. It's a game of cat and mouse that never ends. A decent anti-spam filter such as SpamFighter will hope to stop about 90% of spam, which is great, but that means 1 in 10 are still going to hit your inbox and present you with a security risk that could infect your machine with a virus. You need to be sufficiently aware of what to look for so you can protect yourself directly.

What to look out for

Think of spam emails simply as vehicles to deliver a virus to your computer. The virus will present itself in one of two ways:

1. As an email attachment (a zip / word / excel file for example)
2. The email will contain a link which, when you click on it, takes you to a web page that delivers the virus that way – do read our Ransomware special for more on types of virus

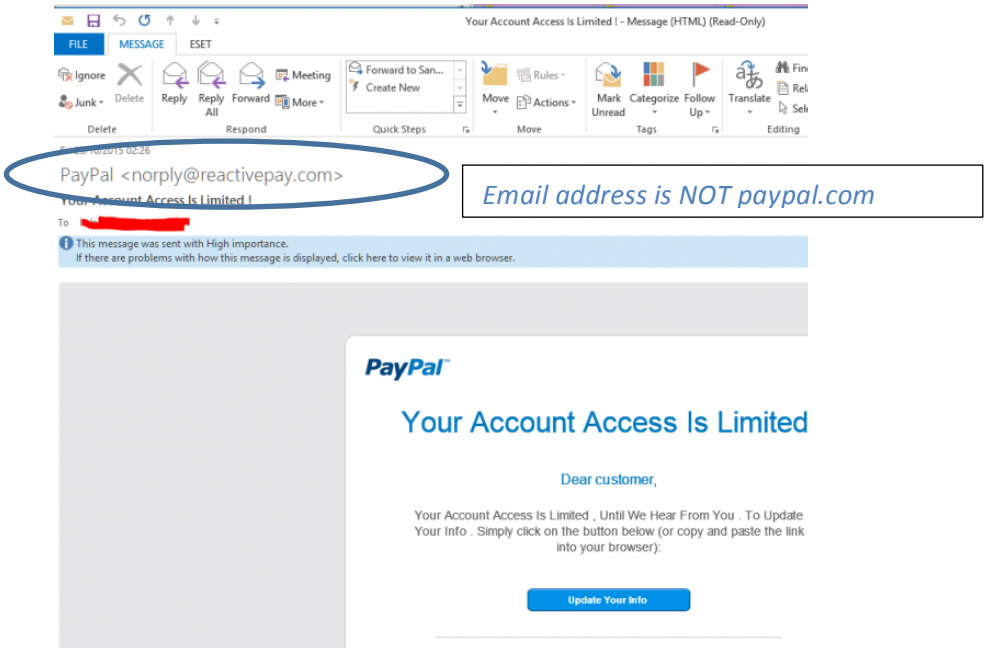
The point is that, on their own, spam emails don't hurt you. They require an action from you to initiate the infection, and this is where you can be smart. Do not click on links in an email. Do not open attachments from a person or company you do not know.

Spotting a fake email versus a genuine one

Spammers are clever at making spam email look genuine (a technique known as spoofing). But there are two simple checks you can do to quickly identify is an email is spam or not:

1. Look at the FROM Address and Domain carefully

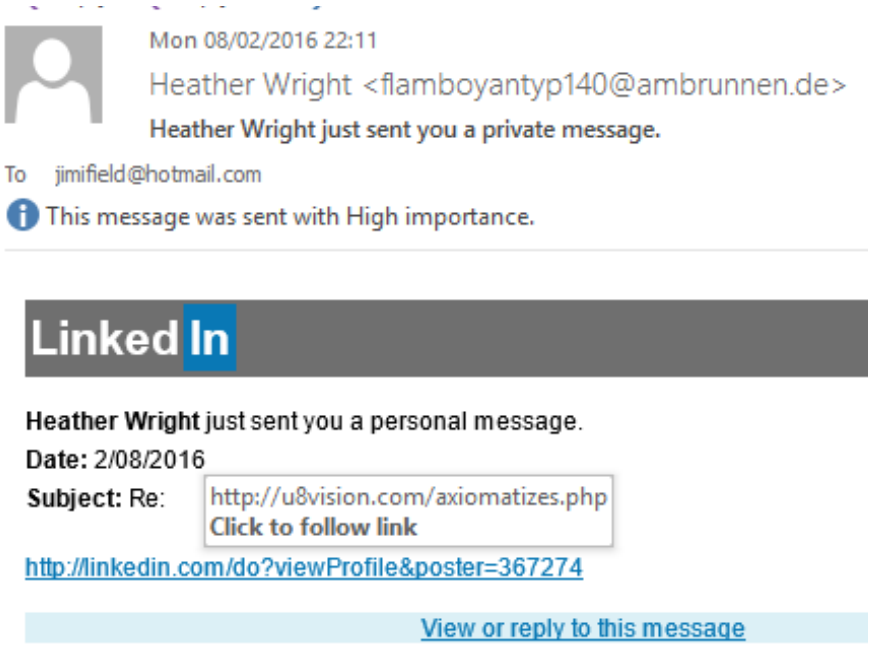
Look at the example below – the email looks like it's from PayPal – same logo, same fonts – but look at the email address it's come FROM. It is not suchandsuch @ **paypal.com**, which is PayPal's genuine domain. It's come from <*norply@reactivepay.com*>, nothing to do with PayPal. Spammers can't send from a genuine domain like paypal.com because they do not own those domains. Any email you get where the sender's domain does not match the exact company domain they are pretending to be from, should be deleted.



2. Check links before clicking by moving your mouse over a link and look at what comes up.

The other simple check you can do is hover your mouse over any links or buttons in the email. DO NOT CLICK THEM, just hover over it. You will see a pop-up appear, showing you what website it would take you to, if you were to click on it.

Look at the below screenshot. It's a spoofed LinkedIn email, and again it looks genuine, but there are telltale signs that it's fake. First of all, look at the FROM address again – it's from a domain called *ambrunnen.de* – nothing to do with LinkedIn whatsoever. But also, when you hover your mouse over the link in the email, which looks like it is linkedin.com, you'll see that if you were to click it, you will actually be directed to http://u8vision.com/axiomatizes.php which will be a virus site. DO NOT CLICK IT! Just delete it immedaitely.



Our Conclusions

Even today, the number 1 cause of viruses successfully infecting computers is the user being duped into clicking a link in a spam email, or opening an email attachment, and granting the

virus permission to wreak havoc.

The best virus and spam protection in the world still is not perfect and therefore you must be aware of what to look for - **you** are the last line of defence!

These simple checks, along with a general cautiousness when using email, and taking an extra few seconds before you click a link, will protect you. And remember, if there is even a *minute* doubt in your mind about the legitimacy of an email, just delete it and pick up the phone – no harm done

Further Reading

Ethical IT's free guide to Ransomware – a really nasty new type of virus often delivered by

Spam emails: http://www.ethicalit.net/resources/Whitepaper-Ransomware-V2.pdf

General article about email safety: https://www.getsafeonline.org/protecting-your-computer/spam-and-scam-email/

The Ethical IT Knowledgebase, with lots of information on topics like PC maintenance, Moving offices, Internet connections and more, all totally free: http://www.ethicalit.net/knowledgebase.php