

Business Plus Article – Jan 2006

Spear Phishing

Why the user can be the weakest point of your network security

We are all familiar these days with junk mail. Previous articles in this column have looked at reducing Spam. Increasingly though, this unsolicited email has moved from harmless if annoying adverts for pharmaceuticals and intimate cosmetic surgery, into the realms of organised crime.

The concept of Phishing has been around for a while. The idea is to send an official looking email, with a plausible request and entice you into divulging your bank details.

The earliest Phishing email I remember was from the son of a deposed dictator in an unstable African nation, claiming to need help in transferring millions of dollars, embezzled while in power, out of the country. All I had to do was give him my bank details and he would transfer all his millions into my account, then split the money with me when he escaped in a canoe down the Zambezi.

While it is possible that I missed a golden opportunity make some fast money, I remained sceptical, suspecting that the money may flow the other way as well.

Nowadays, most phishing attacks are based on a less dramatic approach. They usually claim to be from your bank or credit card company, checking that your account details and PIN are up to date. Some of these can look very official, though most are betrayed by an amazingly poor use of English.

Increasingly, the Phishing technique has been used to deploy viruses aimed at scouring your computer for useful details. These may be dressed as news alerts, undeliverable emails, naked pictures of celebrities, or anything else that might trick an unsuspecting user into opening it. Rather than simply trashing your computer, as viruses did in the good old days, many of them now scour the computer looking for saved details, or simply lie in wait, for you to log into your online banking, before sending your details back to its master.

More recently, however, Phishing has taken a new direction, which is far more dangerous to your business.

Let's be honest. If your users are daft enough to type their bank details into a web page at the request of a poorly written email, it is their lookout but what if they received an email purporting to be from your own IT department. This is a process that has become known as "Spear Phishing".

Suppose it says that they are doing some upgrades to the computer system out of hours, and they need to be able to log in and test that your computer is still ok. They therefore need your username and password to do so. Why bother hacking a network when you can just ask the users for their password?

Once they have this, they could potentially connect to your system, and access confidential information or worse still use your own financial system to get bank details or even transfer funds.

Maybe they don't even need to access the network. How about a mail from an employee to the payroll department informing them that they have moved their bank account and please could you pay their salary into this one instead?

If an email looks to have come from the MD, asking them to pay an invoice urgently, how many people would question it before they paid it?

So how do you guard against this? The first line of defence has to be user education. Make your people aware of the threat, so they do question it. Make it clear that such requests will never be sent by email and need verbal confirmation.

Ensure you have a good Virus scanner on your email system. This should block most of the viral phishing attempts.

Some Anti-Spam products, such as Mail Essentials from GFI software, have Anti-Phishing modules that can spot emails that are not from whom they claim to be, or emails asking for things they shouldn't.

The latest Service pack for Microsoft Exchange 2003 also includes some Anti-Phishing functionality, allowing companies to easily publish a list of their genuine mail servers, so that the system can identify a false sender.

Like any threat, forewarned is forearmed. Be aware of the issue, bolster your protection against it, but most importantly, alert your staff and ensure that your procedures don't leave you open to abuse.

David Wallis
Raven Computers Ltd