

NeoComm is proud to produce its first bi-monthly newsletter. By providing this newsletter, our aim is to inform and educate our clients and associates, of interesting security articles, case studies, dates of interest plus other topical information. Employees of NeoComm are always looking for new ways to improve and continue our professional services to you, so we welcome any comments you may have.



Let's go Phishing

Phishing is a relatively new form of online fraud. In a nutshell, the fraudster running the scam sends out a large number of emails to completely random addresses, typically purporting

to be from some bank, investment house, but could also be any other online business. The email requests that the recipient log into their account with the online business by clicking on a URL embedded in the email message. While the URL may look like the real McCoy, it usually redirects the recipient to a copy of the real website hosted on a machine that has already been compromised. The unwitting user

"Phishing scams have proved to be incredibly effective"

then enters their username and password on the site, which is recorded electronically by the fraudster who then proceeds to transfer funds out of the recipients account.

Phishing scams have proved to be incredibly effective. All the fraudster has to do is get usernames and passwords for a handful of internet banking customers for example, and they could easily net themselves booty in excess of \$10,000.00. With those kinds of odds, phishing scams have attracted the attention of talented programmers and organised crime syndicates, creating more technically sophisticated and targeted scams.

The traditional phishing scam using email has now evolved into a more sophisticated and organised scam, which utilises other techniques to install malicious code, change configuration settings and perform other pervasive actions in order to direct unwilling participants to the fraudsters websites. A new term, 'pharming', has been adopted to identify these techniques.

continued page 2

Security News bits

'Reuters hit by IM worm, network shut down'

Global news and information company Reuters Group Plc said recently, its privately controlled instant messaging service was back in operation after a temporary shutdown triggered by a computer worm.

Read more... <http://itvibe.com/news/3459/>

'Banks 'wasting millions' on two-factor authentication'

Encryption expert Bruce Schneier says, banks are wasting millions of dollars on two-factor authentication, and that the approach is no longer effective. Mr. Schneier says threats have changed since the scheme's invention decades ago, and that it does not protect against modern attack techniques. One such attack is the man-in-the-middle attack, where attackers lure victims to fake websites.

Read more... http://www.theregister.co.uk/2005/03/15/2-factor_auth_is_pants/

'IT the 'whipping boy' for security breaches'

IT departments can end up being the whipping boy for security breaches if they don't drive a cultural change within their organisation, IDC warned last week.

Read more... <http://www.computerworld.com.au/index.php/id;536834811;fp;512;fpid;6625415>

Dates of interest

AusCERT 2005

22nd – 26th May 2005, Gold Coast

<http://conference.auscert.org.au/conf2005/index.html>

International Computer Security Day

30th November 2005

<http://www.computersecurityday.org/>

continued from page 1

According to the Anti-Phishing Working Group (APWG), there were 2625 phishing websites reported in the month of February alone, with an average monthly growth rate of 26% since July 2004.

Unfortunately, there is no simple method by which these types of scams can be stopped. Even two-factor authentication and biometrics, while certainly making the execution of a phishing or pharming scam more technically challenging, do not promise to completely prevent these attacks from being successful. There are two primary issues that contribute to the success of these attacks; low general user awareness and the delays in shutting down phishing websites.

Some key things to look out for and avoid being caught by a phisher:

1. **Never click on a URL sent in an email.** Always type in the URL directly into your browser;
2. **Think about the email you have received before acting.** Is it something you have received before? Were you expecting it? Does it resemble the typical professional communication you receive from your bank or other online business?
3. **Always make sure you are running anti-virus software** and have the latest anti-virus updates installed;
4. **Regularly change your password.** This can help limit the damage;
5. **If you suspect you have received a phishing email,** alert your bank or other online business.

Useful links...

<http://www.antiphishing.org/>

<http://www.netalert.net.au/01604-How-to-avoid-a-Phishing-scam.asp>

http://www.dcita.gov.au/ie/publications/2004/may/phishing_-_dont_take_the_bait!_-_fact_sheet

http://www.oecd.org/document/50/0,2340,en_2649_22555297_33732274_1_1_1_1,00.html

<http://www.scambusters.org/>

Staff Profile

Mark Sayer, Principal Security Consultant and founder of NeoComm Pty Ltd.



How long have you been in the IT industry?

I have been working in IT for ten years, and have held roles including data centre operator, system administrator, systems architecture analyst and security consultant.

Tell me something interesting about your background before IT?

I first caught the IT bug when I was 15 years old. I started out playing games, but soon got bored with them so I started modifying them. Deciding I was destined to be the world's greatest programmer, I started university at RMIT studying computer science. But, while I was happy writing back doors into the Solaris login program, my lecturer wanted me to write programs to simulate a bus going around in circles all day, picking up and dropping off passengers. So after two years of that I decided a career in programming was not for me.

What was your first job in IT?

I was a computer operator, working night shift loading tapes, unloading tapes, loading tapes and then unloading the tapes again. Sometimes I got to do a back-up, but before I could do that, I'd have to load a tape.

What do you do when you're not working?

I'm totally obsessed with sailing and currently race twice a week. At present, I'm trimming the headsail and spinnaker on 'Smooth Criminal', a highly modified Reichel Pugh 36. Essentially, it's a 36 foot windsurfer that goes like a rocket!



What are your interests?

Sailing, and when I'm not sailing, I like to watch sailing videos and read sailing books. If time permits, I also enjoy cooking and showing off my culinary skills to friends and family, travelling, and believe it or not, my work.

Case Study



South East Water (SEW), one of Victoria's largest water suppliers has recently rolled out NeoComm's Security Awareness Training to their staff. SEW's Chief Information Officer,

Mr. Marcus Darbyshire, was able to give some insight into their security issues.

Before the training, Marcus was concerned that, "staff were unwittingly exposing the company to information security threats and potential fraud." To mitigate this risk, SEW had previously carried out security awareness training for their staff over the past two years. Traditional Powerpoint presentations were used, along with security training videos. Marcus believes that, "while both methods were reasonably effective, the training needs to be different each year to hold staff interest." According to Marcus, the benefit NeoComm's security training provided was a reduced exposure to security threats.

Specifically, NeoComm's Security Awareness Training provided staff with a "better comprehension of security threats and wider understanding of information security principles."

SEW found the response rate to the training to be very good, having 60% of staff completing the training in the first two weeks.

One method that SEW used to increase the response rate was to hold a raffle. Eligible entries had to have completed the training within a specified time frame.

As far as the implementation of the training went the software was installed with no interruption to other business services and in minimal time. The ability for users to access the training from the intranet meant that people working from remote sites were also able to benefit from the training quickly, and with no major disruption to their normal activities.

Since the training has been implemented, staff are reporting more potential security incidents to IT, have become more receptive and understand why security controls are important, saying that, "although the security culture has improved somewhat, ... we're never complacent about information security."

When asked whether Marcus found value in the training his response was, "absolutely – well worth it when you consider the cost of potential security incidents. "The NeoComm training package comes highly recommended."

"The NeoComm training package comes highly recommended."

About us

NeoComm is an established Australian protective security consultancy firm with a solid reputation for delivering quality services that are exceptional value for money.

Just some of the many services NeoComm provides are;

- Penetration Testing
- Physical & Information Security Review
- Security Awareness Strategies & Training
- Vulnerability Assessment
- Risk Assessment
- Security Policy Development
- Web Application Security Architecture.

We can tailor a service to your needs, so contact us today.

Contact us

t: 61 3 9894 7720

e: info@neocomm.com.au

Visit our website <http://www.neocomm.com.au/>

If you know of anyone who might like to receive our newsletter, please forward their email address to us. Naturally, we will keep theirs and your information strictly confidential.

To unsubscribe click here.

Or send an email to info@neocomm.com.au with unsubscribe in the subject.