

Mark Anthony Germanos

From: Mark Anthony Germanos [mag@cameronparkcomputer.com]
Sent: Tuesday, August 14, 2007 8:04 PM
To: mag@cameronparkcomputer.com
Subject: How to avoid Social Engineering and Phishing Attacks

You are receiving this email from Cameron Park Computer Services because you purchased a product/service or subscribed on our website. To ensure that you continue to receive emails from us, add mag@cameronparkcomputer.com to your address book today. If you haven't done so already, click to [confirm](#) your interest in receiving email campaigns from us.

You may [unsubscribe](#) if you no longer wish to receive our emails.



How to avoid Social Engineering and Phishing Attacks

Let us run your network while
you run your business
August 14, 2007

Dear Mark,

Watch out for *Social Engineering* attacks and *Phishing* attacks. I will describe them here and also show how to identify when someone is waging one on you or your company.

Opening Notes

- Opening Notes
- Avoid Social Engineering Attacks
- Avoid Phishing Attacks
- Watchguard Certified System Professional - Firewall

Avoid Social Engineering Attacks

In a Social Engineering attack, an attacker gains personal or corporate information in hopes that this information will reveal clues of somebody's personal information or passwords. This would include names of spouses, kids and cars. Attackers use this information when attempting to guess passwords.



My first client was a 1/4 Billion dollar venture capital firm in Chicago. The Chief Financial Officer was married to a man named Timothy. Guess what password she set on all the firm's corporate accounts...Timothy. An attacker with this minimal information could have hacked into their online accounts to defraud the firm.

This presents two solutions. First, be very cautious when revealing any personal information. Second, make passwords hard to guess.

Opening Notes



Identity Theft is the fastest growing crime in our country. Thieves utilize Social Engineering and Phishing in pursuit of stealing our identities.

U.S.-CERT routinely produces valuable advice on computer matters. I am linking to an article produced by Mindi McDowell at the U.S. Computer Emergency Response Team.

[Read on...](#)

Quick Links...

[Newsletter Archive](#)

[More More More](#)

Avoid Phishing Attacks

Phishing Attacks have two theaters. First, the phisher sends bulk e-mail encouraging the reader to click a link and enter personal information. This information could include charge card account numbers, social security numbers and passwords. Second, the link would actually take the reader to a counterfeit site. The user would think this is a legitimate site and enter their valid information. The phisher collects this information and then rips off the user.

I've seen countless messages claiming to be from Wells Fargo, eBay and PayPal. These warn that the reader has to click the link and then enter account usernames and passwords to avoid account suspension.

These links take users to counterfeit web sites. If you type in your valid Wells Fargo, eBay or PayPal account numbers and passwords, the phisher then has easy access to your finances. Do not fall for this trap.

[Read on...](#)

Join our mailing list!
[]**[Join]**

Watchguard Certified System Professional - Fireware



Some have asked what the Watchguard logo and WCSPF after my name mean. These represent the Watchguard Certified System Professional - Fireware certifications I received last Summer. The knowledge I gained while earning these certifications helps me keep businesses like yours in business.

[Read on...](#)

email: mag@cameronparkcomputer.com
phone: 530-677-8864
web: <http://www.cameronparkcomputer.com>

[Forward email](#)

SafeUnsubscribe®

This email was sent to mag@cameronparkcomputer.com, by mag@cameronparkcomputer.com
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).



Cameron Park Computer Services | 3450 Palmer Drive | Suite 4-286 | Cameron Park | CA | 95682-8274