What is this, a change of topic? I’ve gotten tired of network security and am turning to sports news? Or old-time rock ‘n’ roll?

No, not the watery animal, nor the band “Phish:” “Phish” as in “phishing,” the word coined by taking “fishing” and using hacker-style spelling (as in “phreaking”). Phishing is a form of social engineering in which criminals send out spam with forged headers to draw gullible people to fake Web sites where they enter sensitive information such as account numbers, user-IDs and passwords. These data are then used for direct financial fraud or wider identity theft.

I recently received an odd e-mail message that warned me that “my” Wells Fargo account had been closed. Here are the most significant parts of the text with my comments in square brackets:

Dear Wells Fargo account holder,

[Warning sign #1: The salutation is completely general instead of addressing the client by name. The message does not give “my” account number. In any case, I don't have such an account at all (non-account-holders usually just discard the e-mail at no cost to the criminals).]

We regret to inform you, that we had to block your Wells Fargo account because we have been notified that your account may have been compromised by outside parties.

[Warning sign #2: Bad grammar in the warning (the comma between “you” and “that”). Watch for peculiar wording and bad spelling. Now, authentic messages may also have such rubbish, but it’s rarer than in spam – especially spam written by non-native speakers of English. A good deal of the phishing spam is international.]

. . . .

Please be aware that until we can verify your identity no further access to your account will be allowed and we will have no other liability for your account or any transactions that may have occurred as a result of your failure to reactivate your account as instructed below.

[Warning sign #3: Wait a minute: this makes no sense at all. If the account has been blocked, there should be no new transactions allowed, so what liability are they talking about?]

. . . .

Please follow the link below and renew your account information

https://online.wellsfargo.com/cgi-bin/signon.cgi
[Warning sign #4: I immediately went to VIEW SOURCE in my e-mail client to check the URL. (NEVER click on a URL from a stranger without knowing exactly what it is – and its appearance is no guarantee of where it takes you.) Here is the HTML showing the _actual _URL that the fake link went to:

```html
<A href="http://online_wellsfargo_com_account.rndsystems.co.kr:7308/wells.htm"

So as I suspected, the URL in the visible version of the message was just camouflage.]

I hope you will find this simple example and the resources for anti-phishing information helpful; perhaps you can use it for your corporate information security newsletter to help keep your colleagues phish-free.

* * *

For further reading:

Anti-Phishing Working Group (APWG)
< http://www.antiphishing.org/ >

How Not to Get Hooked by a ‘Phishing’ Scam (FTC Alert)
< http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm >

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.