

INFORMATION SECURITY MATTERS

April 2005
Volume 2, Issue 2

Cedric Bennett & Associates • ced@bennettsite.com • 650 858-0883 • <http://bennettsite.com/cba>



Phishing Can Be Bad For Academic Business

“Phishing” is such a cute-looking term. It seems like it ought to be harmless. But let’s not kid ourselves about it — phishing represents a pernicious criminal activity aimed at gaining individual identity information for a variety of purposes including fraud and theft.

Although early versions of this particular scam were almost laughable and not particularly convincing, the sophistication of this type of attack has been rising, making it much more difficult for the average person to recognize what is occurring. Not only do the email “invitations” look extremely legitimate, right down to contact information and small-print copyright notices, but the websites they direct traffic toward also appear very official by carefully mimicking the look of sites they are pretending to be.

Most phishing attacks have been focused on getting the victim to go to a web page in which they are asked to “verify” personal account and other identity information. The

“...phishing represents a pernicious criminal activity...”

How Do We Select Security Products?

In a recent conversation with a vendor of security products, I was asked what the primary motivator was for a higher education purchase of an information security product. I think the question was not really so much about what motivated me or any responsible security officer to buy some product. The vendor

Inside This Issue

Phishing Can Be Bad For Academic Business	1
How Do We Select Security Products?	1

data thus harvested can be used to buy things, cash checks, or even withdraw funds directly from accounts.

But there is another potential and growing target for phishing attacks. This same approach can be used to gather institutional-access information from users of our systems. A criminal intent on gaining access to student data, for example, can send official-looking email to users, directing them through a provided link, to a site where they are asked to enter their university-access information. Such an attack, based upon what many of our institutional email communications already do (and also on the natural trust that users have for our university systems), can easily fool employees into doing as they are asked.

We need to do at least two things at our institutions to head off this potential security breach.

On the one hand, we should continue to raise
Please see **Phishing** on page 2

was really interested in the primary factors that would motivate institutional management to allocate funds for the purchase.

After a carefully worded caveat about anyone’s ability to represent all of higher education thought on this topic (or all of higher
Please see **Select** on page 2

Phishing from page 1

user awareness of phishing attacks, what they can cause in terms of personal loss, and how to avoid them (by not following *any* link which is provided via email where identity verification is requested).

On the other hand, and even more importantly, we should educate our information technology professionals and others to stop providing those helpful browser links in email *where the linked-to site is going request identity or authorization verification*. Our institutional systems have to stop mirroring the very activity that makes phishing so successful.

Instead of providing actual links in such cases we should describe the web navigation necessary for a user to find the appropriate page, starting from institutionally well-known home pages or via established portals. Even though not providing a direct web link might be perceived as a reduction in user-helpfulness, the email describing the navigation information can actually enhance users' security awareness by including a brief explanation of the anti-phishing approach being followed. ♥

Select from page 1

education thought on any topic) I offered my opinion.

What I wanted to be able to say was that our institutions were motivated by strategic opportunities with regard to information security and that the product which both fully addressed the issue of concern and also promised the widest set of additional capabilities would be the hands-down winner. I wanted to add that even if the better product had a price premium attached (justified because it provided so much additional useful capability) it would be seen by our institutions as the overall, long-term, better approach.

That's what I really wanted to say.

What I did say was that security products are, for the most part, providing a "negative benefit." That is, when they do what is desired, the result is that something bad doesn't happen (or at least it happens less frequently or less severely). Like insurance, we spend money on security products as a protection mechanism against potential future problems. Unlike insurance, however, which pays off in dollars designed to help the insured replace or fix whatever was damaged if the bad thing happens, successful security products are measured by what *doesn't* happen.

This fact of life about security products automatically makes them a very tough sell within our institutions (see *Information Security Matters*, "*Information Security Can Be a Very Tough Sell*," January 2005, Volume 2, Issue 1 for a related article). To the vendor who asked this question, I opined that most institutions would at most agree to buy the product that zeroed in on the particular pain-point that was being addressed and only at the most reasonable price. I added that if one product had additional and useful functionality those factors would be an important consideration in choosing that vendor's product over another but the vendor should not expect such non-requested value-added functionality to support a premium price.

Days later, I thought more about this conversation and decided to share it with readers of this newsletter and to also ask for your opinions on the topic. I'm sure nearly all of you have an opinion - I hope some of you are willing to share it with me. Please email your comments to Ced@Bennettsite.com. I'll take all the input I receive on the topic and summarize it in the next issue (without revealing any respondent's identity). ♥