CNS /Update Newsletter Feature

Phishing Scams -- An Ongoing Threat to UF

CNS Document ID: U0810-phish
Last Updated: 09/23/2008

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

Phishing Scams -- An Ongoing Threat to UF ..............................................................3
Phishing Scams -- An Ongoing Threat to UF

It's the start of a new academic year and thus good to reiterate some external risks and security practices essential to protecting our critical information resources and personal identification information. Like all large universities, UF is a prime target for phishing scams that can be used to compromise GatorLink accounts. Compromised accounts can potentially be used to access your personally identifiable information and other protected data resources.

While UF email filters block large portions of phishing attempts, scammers are constantly adapting their tactics to bypass filters. The highest level of protection requires constant vigilance and care on the part of end users. It is incumbent upon you - the email recipient - to be aware of scams. Here are some good practices to incorporate in your routines of using computing resources:

• Don't click on the web links found in email
• Never provide your password to ANYONE
• If you think you've been a victim of scam, change your password immediately.

Scammers cleverly try to impersonate a trusted source such UF IT staff. To avoid being duped, NEVER respond to email asking for your personal information, even if appears to come from a trusted source such as UF IT workers. Scammers are also crafty about luring people to phony web sites that look just like the real thing. To be safe on the web, NEVER follow links found in email. Instead, manually enter the web site name or use your favorite search engine.

• ACT IMMEDIATELY if you've been "phish-hooked." For UF accounts, contact the UF Helpdesk at 352.392.HELP or helpdesk@ufl.edu.
• PLEASE REPORT SCAMS even if you haven't responded to a suspicious e-mail. At UF, report any suspicious e-mail to abuse@ufl.edu.

For up to date information about scams that are targeted at UF users, see http://infosec.ufl.edu/blog/category/advisories. To learn more about phishing scams, see http://infosec.ufl.edu/athome/phishing.shtml.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology
UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>