Physical Plant IT Spoofing Test

- Why we did it
- What we did
- Who we duped
- What we learned
- What we really learned
Noticed correlation between phishing emails and “forgotten” passwords by users

Warnings did not help
Physical Plant IT Spoofing Test

- Met with PPD Administration
- Met with Infosec
- “Low key”
Subject: Notice: Human Resources needs your assistance in order to process your IRS Payment Checks
Date: Mon, 14 Apr 2008 12:01:58 -0400
From: UGA Human Resources <ugahr@gmx.com>
To: UGA Human Resources <ugahr@gmx.com>

Dear UGA Employees,

We apologize for this late notice but due to the nature of which the IRS is pushing out the Economic Stimulus Payments, we require you to verify and update your employee information. If you do not check this information, you may be delayed in receiving your check.

Please visit this site to verify and update your information
UGA Human Resources <http://tinyurl.com/5n3ras>

Please double check your information before the end of Tuesday, April 15th, 2008.

More details can be found about the Economic Stimulus Payment here:

Economic Stimulus Payment <http://tinyurl.com/2z7wf5>

Starting in May, the Treasury will begin sending economic stimulus payments to more than 130 million households. To receive a payment, taxpayers must have a valid Social Security number, $3,000 of income and file a 2007 federal tax return. IRS will take care of the rest. Eligible people will receive up to $600 ($1,200 for married couples), and parents will receive an additional $300 for each eligible child younger than 17. Millions of retirees, disabled veterans and low-wage workers who usually are exempt from filing a tax return must do so this year in order to receive a stimulus payment.

Thank you for your prompt response,

UGA Human Resources Department
uga myID verification

MyID:  

Password:  

Due to a change in our payroll systems, we must verify your MyID and password. This is necessary to ensure that you will correctly receive your pay.

Click here for supported browser information.

Forgot your password?

Logon
Over 100 Physical Plant employees “attempted” to login
EITS notified PPD IT of PPD Server “compromise”
Employees talk to other departments
Follow-up training required for duped users
Physical Plant IT Spoofing Test

- Users will believe visual cues
- Money/paychecks get attention
- Previous warnings sent just two days prior to spoof site going live had little (no?) effect
- Word-of-mouth cut into our duped numbers
Physical Plant IT Spoofing Test

INVOLVE EVERYONE!