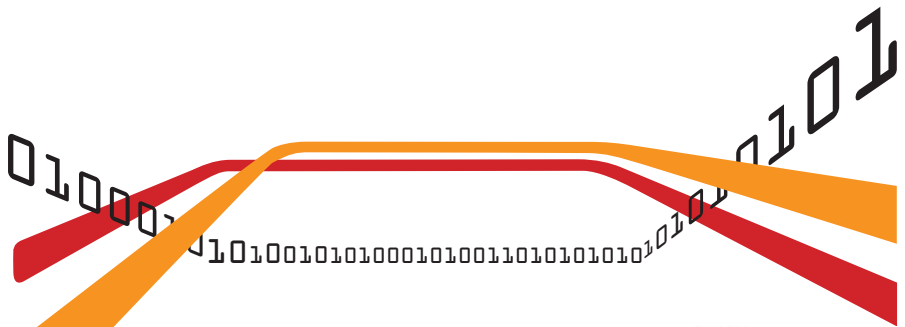



R·I·T

Information Security Field Guide to Identifying Phishing and Scams



INFORMATION
SECURITY



0100010101001101

Contents

Introduction

Phishing

Spear Phishing

Scams

Reporting

Resources



Introduction

00101000101001010



Welcome to the RIT Information Security Field Guide to Identifying Phishing and Scams. This guide will help you determine whether something you've received is authentic or whether it may be a phishing attack or scam. RIT always sees a number of phishing attempts that try to trick the recipient into disclosing login credentials—username and password. Although the intent of the phishing attacks normally appear to be to enable attackers to use the accounts to send out additional spam and phishing emails, attackers may also try to gain access to and steal or alter RIT Confidential Information. Attackers may also gather account information to help them commit identity theft.

The RIT Information Security Field Guide to Identifying Phishing and Scams provides examples of common phishing, spear phishing, and scams that are common in higher education. The Guide also provides the steps to take when you've encountered one of these attacks.

Remember, RIT will never ask you for your password. It's not needed to reset your account.



Phishing

Phishing attacks are typically emails sent to a wide target audience with the intent of acquiring login credentials, account numbers, Social Security numbers, or other Private Information. The goal of the attackers is to commit Identity Theft. Although it used to be quite easy to identify the attacks because of poor grammar and other “tell tales,” the attacks have become more sophisticated. It’s now possible for an attacker to purchase tool kits to create high quality phishing attempts.

The 2015 Symantec Internet Threat report (http://www.symantec.com/security_response/publications/threatreport.jsp) estimated that 1 in 965 emails were phishing attacks. You will see similar phishing attacks, both at RIT and at home.

The example is from <http://www.millersmiles.co.uk/email/please-login-to-update-your-account-id-informations-apple>. The key telltales are the generic salutation and malicious link.

10100110010101001010010100100100100100





Phishing Example

This is an automated email, please do not reply

DEAR CLIENT

We've noticed that some of your account information appears to be missing or incorrect We need to verify your account information in order to continue using your Apple ID, Please Verify your account information by clicking on the link below

CLICK HERE TO VERIFY YOUR ID

Thanks for choosing Apple,
Apple Team

Â© 2015 Apple. All rights reserved.

Email ID: 163327

...

Generic

Link to malicious website





Spear Phishing

Spear Phishing attacks target specific groups. The groups may be large (Hilton Honors members) or small (a specific department or individual). Spear phishing is more difficult to identify than a typical phishing attack. The email may be addressed to you specifically and may contain information that makes it appear to be valid, such as information that pertains only to the target audience. The links, although masked as in the phishing example, often go to websites that mimic an official website. (Remember, the use of institutional branding on the website does not mean that the website is legitimate.) The emails may also have malicious attachments.

In the example on the facing page, callouts identify some of the telltales that make it easier to identify the suspect email as a spear phishing attempt. These telltales include use of a generic addressee, spelling errors, and a link that goes to an external website. (Identify where a link actually goes by hovering your cursor over the link. You'll see a pop-up like the one in the example. Note: The hover technique may not be usable when on a smartphone.) You'll also see that the sender "Edu Help Desk" is a generic sender not associated with RIT. Additionally, the RIT Information Security Signature Standard requires sufficient contact information for the sender to establish that the email is legitimate.

10100110010101001010010100100101001010010100



Spear Phishing Example

Ben Woelk

From: Edu Help Desk <info@pa.com>
Sent: Tuesday, September 08, 2015 3:16 AM
To: info@pa.com
Subject: [Suspected Spam] Edu Email Upgrade Against Spam.

Attn: Email User.

Due to the high risk of spam emails going on in the internet, we have decide to upgrade all educational email set by our admin panel, and access to your mailbox via our mail portal will be unavailable expect you upgrade your email account against fraudulent spam.

To upgrade and re-validate your mailbox, do click on the link to upgrade: [Upgradepage](#)

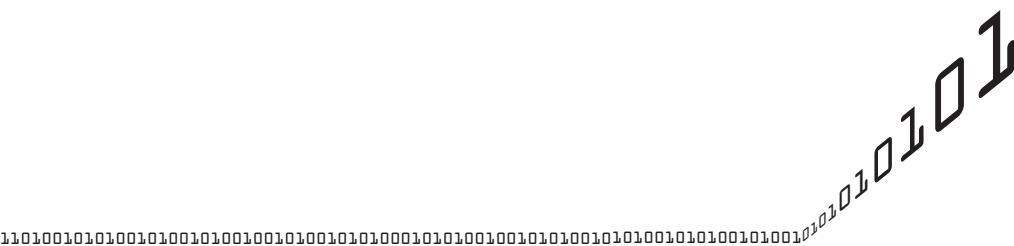
Thanks,
Educational Ad

[http://www.designrepublic.cz/
wp-content/advanced/cache/upgrade/
account/webmail.php](http://www.designrepublic.cz/wp-content/advanced/cache/upgrade/account/webmail.php)
Click to follow link

Spelling

Generic addressee

Link goes to external site





Scams

We've seen examples of many different scams reported at RIT. The scams often involve financial fraud and may be reported by a vendor or detected by the recipient. Here are examples of these scams.

Fake purchase orders

RIT and other university vendors have received fake purchase requests. They may appear to have been sent by RIT, but the address is usually spoofed. The callouts in the example provide some of the telltales. However, this type of attack is hard to detect and depends on the vendor having good internal processes.

Wire transfer authorizations

There are several types of wire transfer fraud. The type we've presented here is an example of a high-level executive's account being compromised or spoofed. The request for a wire transfer is made to a second employee who is normally responsible for processing that type of request. The request is often marked "Urgent." In one recent example, a college in Virginia wired \$1,000,000 to an overseas account.

Protecting against these attacks

In addition to normal spam filtering and good information handling practices, the FBI suggests that businesses include a telephone call or other type of additional verification before approving such requests. They also recommend that employees be alert for sudden changes in business processes.





Fake Purchase Order Example

From: John Doe (<mailto:rollingpoint027@spoofedemail>)
Sent: Friday, May 01, 2015 10:46 AM
Subject: Quotation

Attn Sales:

My name is John Doe on behalf of Rochester Institute of Technology, we would like to order for the below items:

Cisco 1941 - Integrated Service Router - desktop, rack-mountable - CISCO1941/K9
BenQ MX722 4000 Lumen XGA 3D DLP Projector
InFocus IN3124 DLP Projector
Hitachi CPX4015WN CP X4015WN - LCD projector - 4000 lumens
OEM C6578DN Tri Color Inkjet Cartridge

We look forward to hear from our dedicated account rep with a price quote as soon as possible.

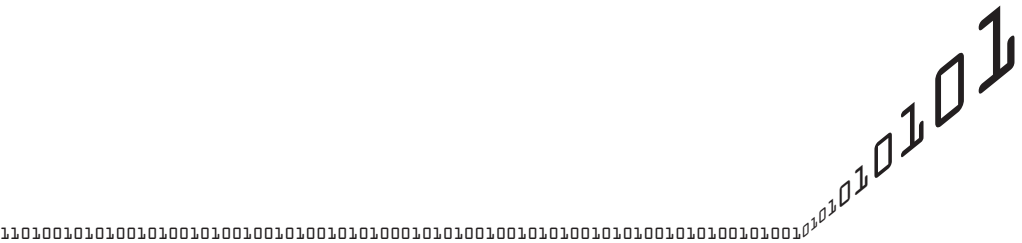
Thanks,

John Doe
Corporate Controller
Rochester Institute of Technology
7 Lomb Memorial Drive
Rochester, NY 14623-5603
john.doe@spoofedURL

Non-RIT email address

Generic Salutation

Spoofed email address





Resources

Cyber-Related Scams Targeting Universities, Employees,
and Students

<http://www.ic3.gov/media/2014/140505.aspx>

Scammers pose as company execs in wire transfer spam
campaign

[http://www.symantec.com/connect/blogs/scammers-
pose-company-execs-wire-transfer-spam-campaign](http://www.symantec.com/connect/blogs/scammers-
pose-company-execs-wire-transfer-spam-campaign)

Cyber Thieves Steal Nearly \$1,000,000 from University of
Virginia College

[http://krebsonsecurity.com/2010/09/cyber-thieves-steal-
nearly-1000000-from-university-of-virginia-college/](http://krebsonsecurity.com/2010/09/cyber-thieves-steal-
nearly-1000000-from-university-of-virginia-college/)

Targeted Wire Transfer Scam Aims at Corporate Execs

[http://blog.phishlabs.com/targeted-wire-transfer-scam-
aims-at-corporate-execs](http://blog.phishlabs.com/targeted-wire-transfer-scam-
aims-at-corporate-execs)

Business E-mail Compromise

<https://www.ic3.gov/media/2015/150122.aspx>

RIT Information Security Identity Theft page

<https://www.rit.edu/security/content/identity-theft>

RIT Information Security Phishing page

<https://www.rit.edu/security/content/phishing>

FTC Recovering from Identity Theft

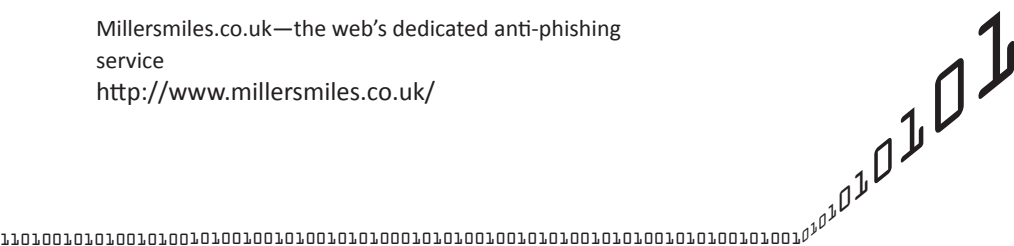
[http://www.consumer.ftc.gov/features/fea-
ture-0014-identity-theft](http://www.consumer.ftc.gov/features/fea-
ture-0014-identity-theft)

SonicWALL Phishing IQ Test

<http://www.sonicwall.com/furl/phishing/>

Millersmiles.co.uk—the web's dedicated anti-phishing
service

<http://www.millersmiles.co.uk/>





R·I·T

digital
self
defense
www.rit.edu/security



Don't get hooked!

NEVER respond to e-mail requests for your password.

get informed

Visit the RIT Information Security website to view additional information on staying safe online.

RIT INFORMATION SECURITY

<http://rit.edu/security>

infosec@rit.edu

(585) 475-4123

September 2015



INFORMATION
SECURITY