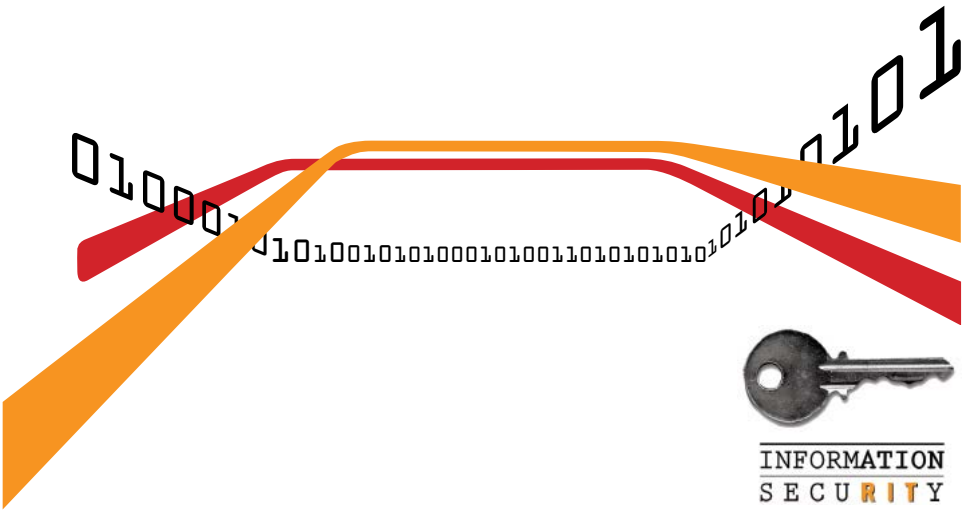
R·I·T

Information Security Field Guide to Identifying Phishing and Scams



Contents

Introduction

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.

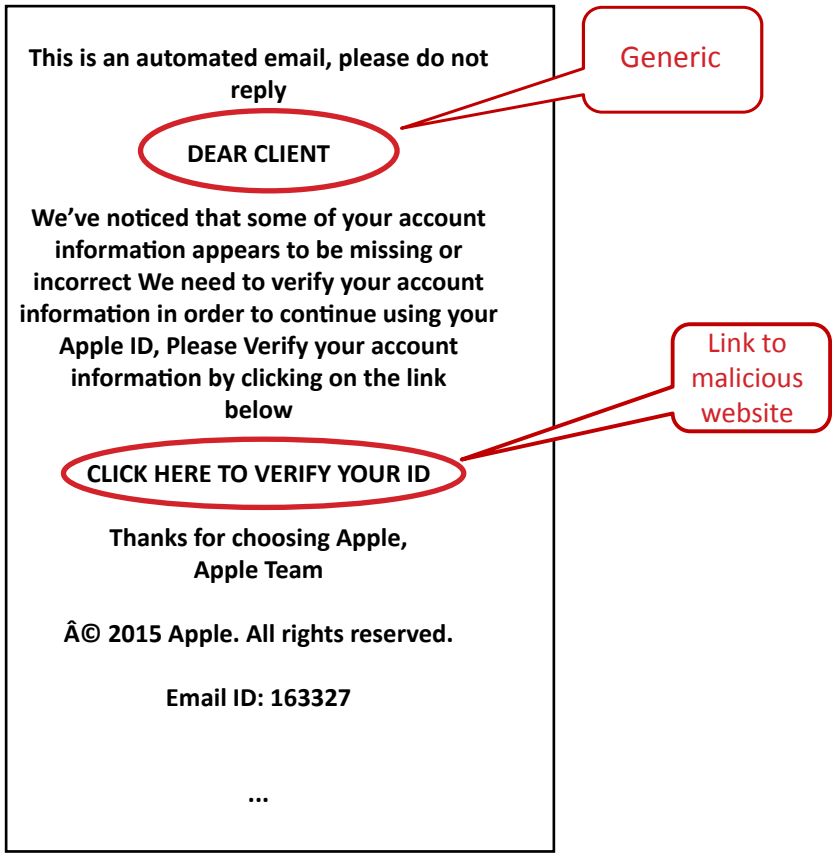
Phishing

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.

Phishing Example

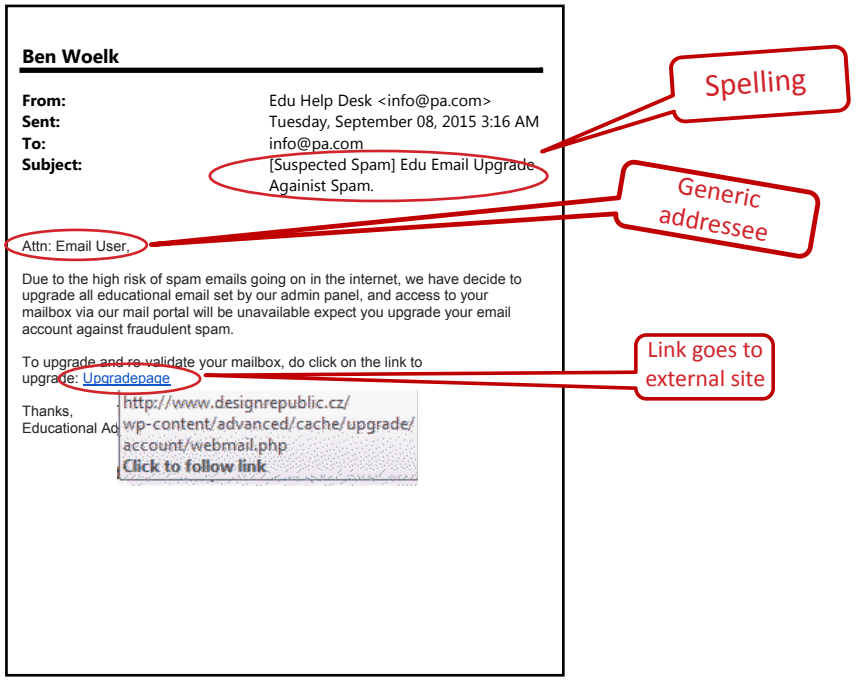


Spear Phishing

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.

Spear Phishing Example



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.

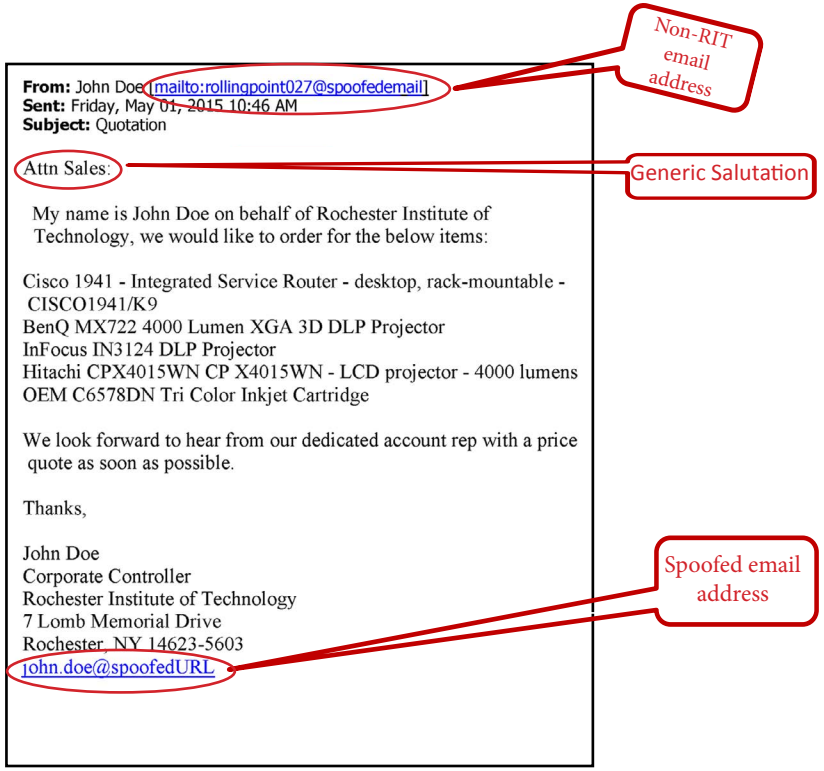
Wire transfer authorizations

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



Reporting

Report generic phishing attacks to spam@rit.edu. (Open a new mail note and insert the phishing email into the new mail note. Then send it to spam@rit.edu.) Delete the phishing email after forwarding it to spam@rit.edu.

Please report spear phishing (targeted) attacks directly to the RIT Information Security Office by sending a copy of the email to infosec@rit.edu in addition to spam@rit.edu or by calling 585-475-4122.

If you believe your account credentials may have been compromised or that you've supplied other information to the attacker, please contact the ITS Service Desk (585-475-HELP).

If you believe you're the victim of a scam, please contact RIT Public Safety (585-475-2853).

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

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/

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/feature-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/

http://www.rit.edu/security

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