E-mail Security: Phishing and Scams.

Teresa Gibbons
ITU Support Center Manager
October 18, 2012

Honey, Get My Tackle Box

- http://www.onguardonline.gov/media/video-0006-phishy-home

Overview

- Phishing
- SPAM
- General E-mail Security

What is Phishing?

- Phishing is a form of social engineering that uses e-mail or malicious websites to solicit personal information by posing as a trustworthy organization.

- It preys on qualities of human nature:
  - the desire to be helpful
  - the tendency to trust people
  - the fear of getting into trouble
  - the concern of losing something (usually access)

What Does It Look Like?

- **False Sense Of Urgency**
- **Suspicious-Looking Links**
- **Not personalized**
- **Misspeld or Pooooorly Written**
- **Sender not known**

Example 1

Subject: REVALIDATE YOUR MAIL ACCOUNT.
From: WEB ADMINISTRATOR <administrator@e-webadmin.co.cc>
Date: 10/10/2012 10:24 AM
To: undisclosed-recipients:;

Dear user,

We wish to inform you that, due to the large amount of spam messages we receive daily in our message center, We have decided to reset our server in order to serve you better. In order prevent limited access to your email account or loosing your email account completely, you are hereby advised to click the link below and fill in the necessary information to revalidate your email account on our database and update your e-mail quota.

http://webudatedesk.ucoz.com/index.html

Failure to revalidate your email account with our database within the next 48 hours, may lead to loss of important information in your mailbox or complete loss of your email account.

Thanks for your cooperation.

Web Administrator

Example 2

Subject: Upgrade your account
From: Educacao Ambiental <ambiental@seduc.to.gov.br>
Date: 10/11/2012 8:34 AM
To: undisclosed-recipients: ;

This is to inform you that you have exceeded your quota limit e-mail and you need to increase the quota limit e-mail, because in less than 24 hours, your account email address will be your disabled.Increase quota limit email and continue to use your webmail account. To increase youe email quota limit of 2.7GB, fill in your details as below and send to Webmaster
Email share by CLICKING REPLY:

E-MAIL:
USERNAME:
PASSWORD:
Confirm Password:
DATE OF BIRTH:

Thank you for your understanding and corperation in helping us give you the best E-mail Service.2012?

Example 3

-------- Original Message --------
Subject: ATM/Debit Card - Reference Number : wn6lLlAxmdzG%
Date: Fri, 03 Feb 2012 13:31:42 +0200
From: ATM/Debit Card <aak10@psu.edu>
To: [redacted]

Dear Cardholder,

We have completed our ATM/Debit Card software upgrade and determined that an error did occur.
It will only take few minutes to re-activate.
Please click the link below to proceed with re-activation process :

http://atm9308885.onlinechase-10p7vv2toeocofq.vaw.does-it.net/us/gmu/index.php?checkcard=cmcdani1@gmu.edu

If you have further questions, please call us at 1-800-548-9554. Our hours are (in Pacific Time):

During Daylight Saving Time: Monday - Friday, 5:00 am - 5:00 pm; Saturday, 7:00 am - 4:00 pm.
During Standard Time: Monday - Friday, 4:00 am - 4:00 pm; Saturday, 6:00 am - 3:00 pm.

Thank you for bringing this matter to our attention. We hope we have been able to assist you.
Sincerely,
Chase Debit Card Operations
You received this notification because you are a cardholder, account owner, or an authorized representative for this account.

What's the Big Deal?

Phishing Attacks Lead to Identity Theft - When users respond with the requested information, attackers can use it to:

- Empty your bank account
- Open new credit cards
- Gain employment
- Give your name to the police during an arrest

More Specific to Mason

Your Mason UserID gives access to:

- Patriotweb / Internet Native Banner
  - Student/Employee Personal information
  - Financial information
- Mason Money
- MyMason
- And much, much, more….

Does Phishing Work?

- The Bureau of Justice Statistics (BJS) estimated 11.7 million persons are victims of identity theft
- That's five percent of all persons age 16 or older in the United States
- The financial losses due to the identity theft totaled more than $17 billion.

http://bjs.ojp.usdoj.gov/content/pub/press/vito8pr.cfm

Don’t Take the Bait

Treat all e-mail with suspicion

Never use a link in an e-mail to get to any web page

Never send personal or financial information to any one via e-mail

Never give out personal or financial information solicited via e-mail

When in doubt forward to support@gmu.edu

What About SPAM?

- SPAM is unsolicited commercial e-mail…which may include phishing attempts, but is often simply unwanted marketing
- Phishing often has criminal intent while SPAM does not, BUT IT CAN
- Treat SPAM offers the same way you would treat a telemarketing call
- Don't believe promises from strangers, if it sounds too good to be true, it probably is

http://www.gmu.edu/depts/itu/tsd/esm/email/spam

SPAM Example 1

Subject: Notification Of Funds
Date: Wed, 6 Nov 2012 23:16:55 PST
From: JMC Marketing <jab1@lists.tilw.net>

It has come to our attention that you may be entitled to an undisclosed amount of unclaimed funds.

If so, these funds are currently reserved in your name and waiting or you to claim.

Please enter your name at the unclaimed money search engine located at our site.
Click Here

Notification Date: 10/15/12 to 11/15/12

Unclaimed Funds Department
Found Money.com

We take your privacy very seriously and it is our policy never to send unwanted email messages. This message has been sent to you because you originally signed up with a party that has contracted with JMC Marketing Concepts.

To unsubscribe click here or go to and enter your email address.

JMC Marketing Concepts
1003 E. Concho
Rockport, TX 78382

SPAM Example 2

Subject: Protect freedom of speech in Russia
Date: Thu, 7 Nov 2011 05:11:53 +0100 (MET)
From: freest@WildEmail.com
Reply-To: phillip@TougherThanYou.com

How to help us Although our organization is based on a non-profit principle, we need money to implement and maintain our projects. We dependent on donations by those who share our concerns and want to help us with our work. Please support us with your donations. We will appreciate any amount you give - 'many drops build a river', so never think that your dona! tion is too small to take action.

Our Bank accounts open for you:

US dollars - ING Bank NV Netherlands: 02.01.99.910
Dutch Guilders - ING Bank NV Netherlands: 68.01.26.988

All information on donations, sponsorship, etc. will be treated in strictest confidence!

If you do not want to publicize any information about yourself, you can make an anonymous transfer to our bank account from any bank office. To
do this just transfer an amount in cash with the remark "donation".

There are various possibilities to work with us which are outlined

Who we are Kavkaz-Center (www.kavkazcenter.org) - is Chechen independent international Islamic Internet agency. Our agency was founded in March of 1999 in the city of Jokhar (Grozny). The founder is the National Center for Strategic Research and Political Technologies, which was ! in turn
registered, with the Ministry of Justice of the Chechen Republic of Ichkeria in October of 1998 (N 1377/A-17).

What is the ITU Doing about SPAM?

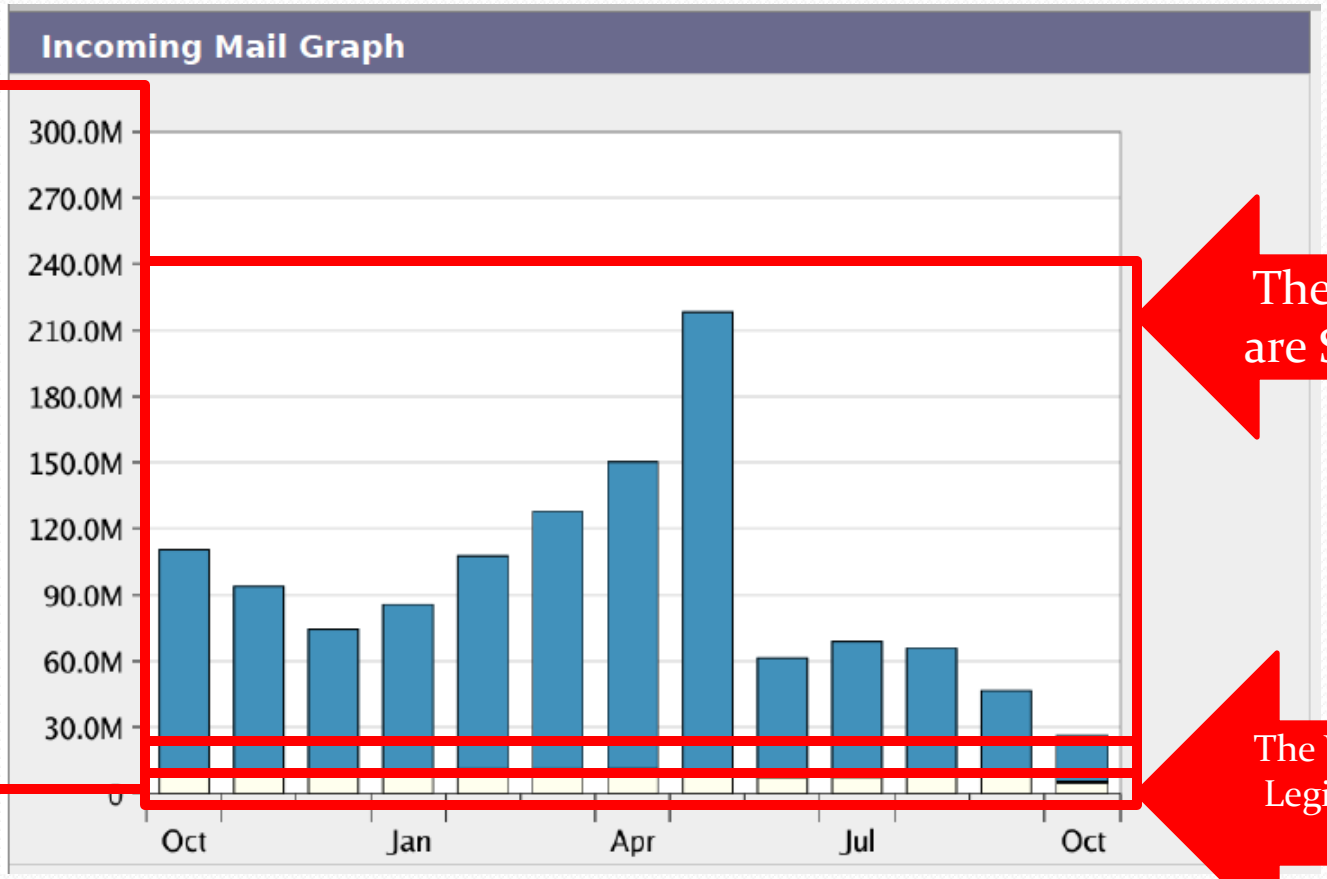
IronPort filters out as much SPAM as possible, it employs an exclusive Context Adaptive Scanning Engine™ (CASE) to examine the complete context of an e-mail message including:

- Content of the message
- Construction of the message
- Reputation of the message sender
- Reputation of the site from which a message is sent

What???

- IronPort scans e-mail messages before they get to your inbox and based on what it knows it blocks most of the junk

Incoming Mail



These are Millions of Messages a Month

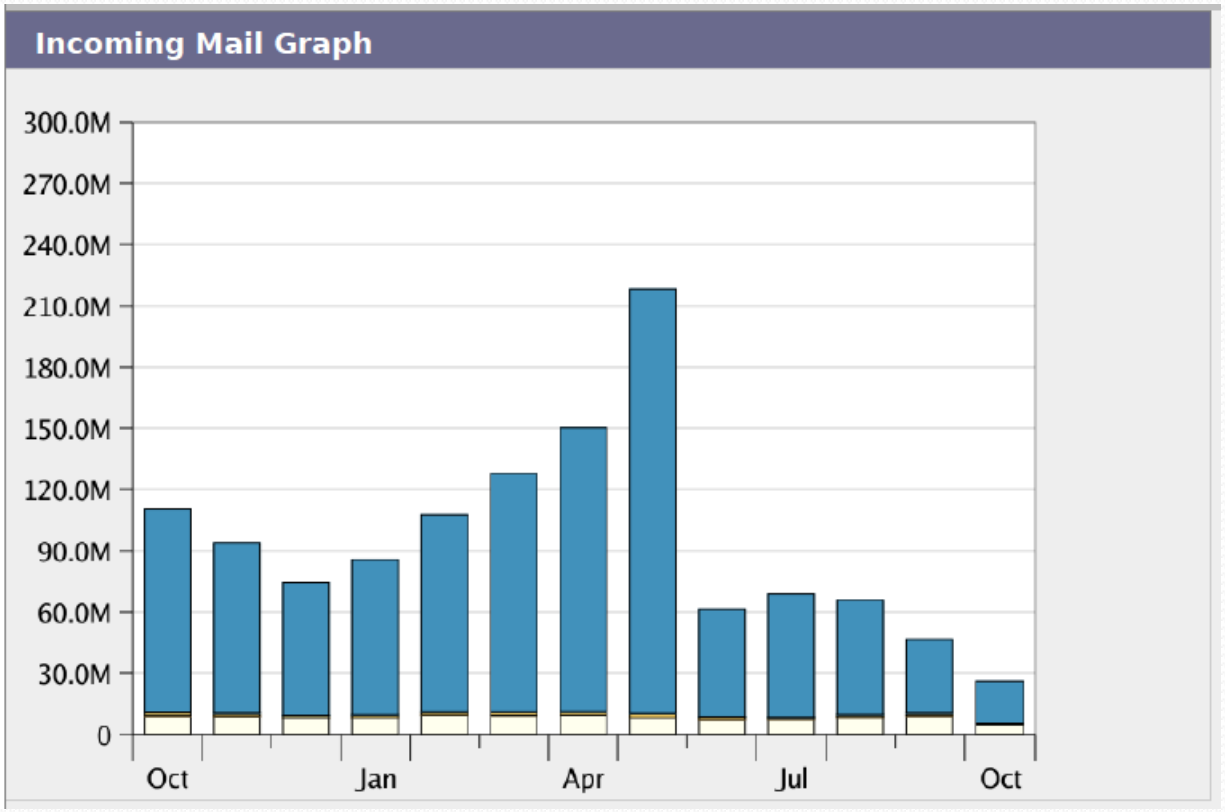
The Blue are SPAM

The White are Legitimate E-mails

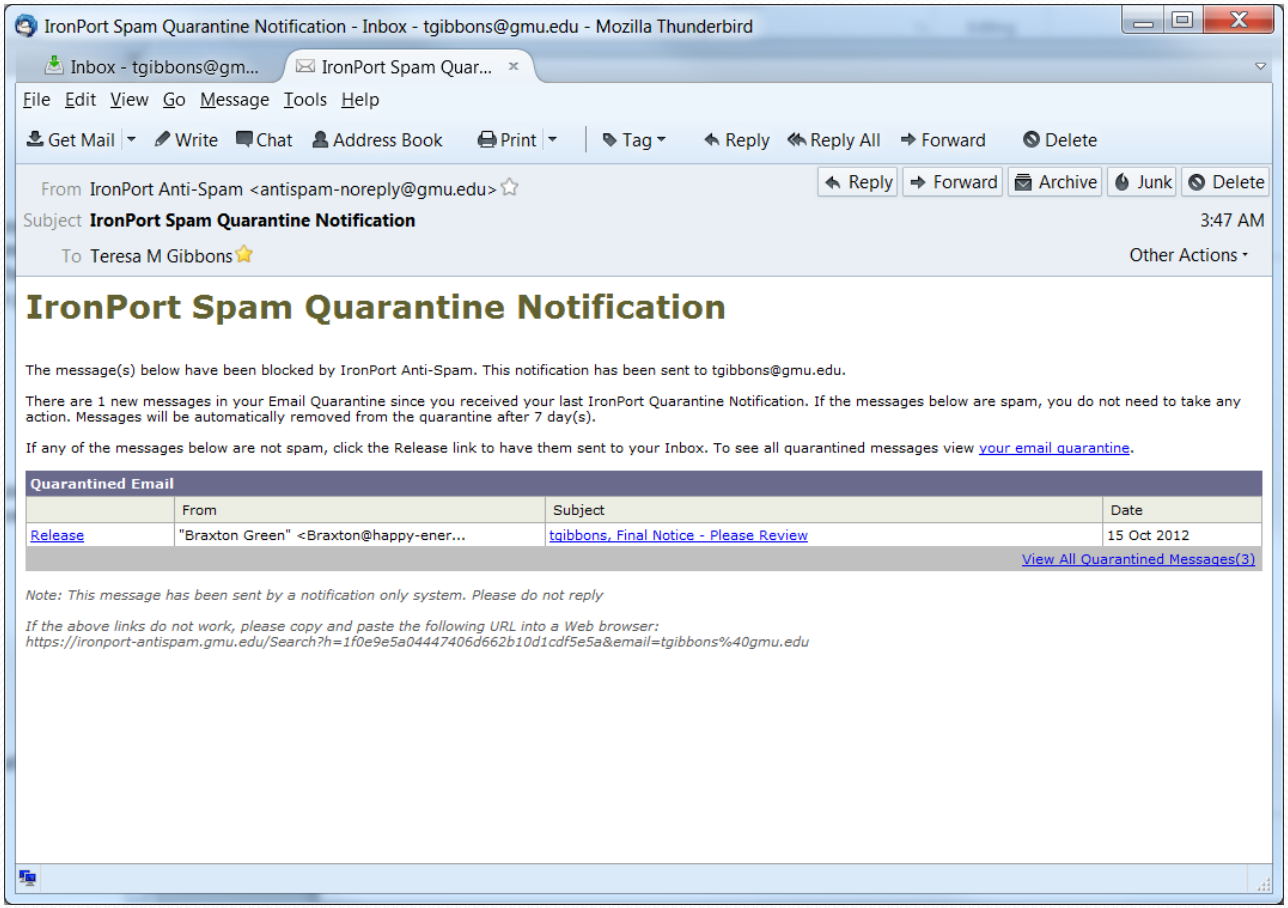
Caught SPAM

Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	89.8%	1,110,339,256
Stopped as Invalid Recipients	0.0%	27,396
Spam Detected	1.4%	17,188,306
Virus Detected	0.0%	47,728
Stopped by Content Filter	0.0%	34,999
Total Threat Messages:	**91.2%**	**1,127,637,685**
Clean Messages	8.8%	109,445,961
Total Attempted Messages:		**1,237,083,646**

Stopped By Filter



Personal IronPort Report



How Can I Protect Myself?

- Be cautious about opening attachments in e-mails
- Be very cautious about downloading files
- Be suspicious of unsolicited e-mails asking for information
  - If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Pay attention to the URL of a website
  - Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

More Protective Measures

- Passwords
  - Do not use the same one for everything
  - Do not write it down
  - Do not share it with anyone
  - Do not make it easy to guess

What to do if you think you are a victim?

- If you think you've been compromised, **immediately change your passwords**
- If you believe you may have revealed sensitive information about George Mason University, contact the ITU Support Center 703.993.8870
- If you believe your financial accounts may be compromised, contact your financial institution immediately then, watch for any unexplainable charges to your account
- Consider reporting the attack to the police, and filing a report with the Federal Trade Commission (http://www.ftc.gov/)

Questions???

Phishing Pop Quiz

What are 3 of the 5 ways of identifying an Phishing Message?

- False Sense Of Urgency
- Suspicious-Looking Links
- Not personalized
- Misspelled or Poorly Written
- Sender not known

SPAM Pop Quiz

How many of these sound like SPAM?

Work at Home Fast Cash, Minimal Work, No Risk!

Turned Down by Banks? Bad Credit? We'll Pre-Qualify You !

Lose up to 2 Pounds a Day with New Miracle Diet Pills!

Wipe Out Debts! Consolidate Bills! Let Us Help!

Additional Information

- http://security.gmu.edu/spam
- www.gmu.edu/email/spam/
- http://www.onguardonline.gov
- http://www.antiphishing.org

Thank You

Keeping you safe. Keeping you secure. Keeping you protected.
Mason.