BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Welcome!

Phishing And Ways To Combat It

Phishing and ways to combat it

Lance Bailey
Systems Coordinator
Genome Sciences Centre

Don Devenney
Information Technology Analyst
Royal Roads University

Phishing

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims.

-- techtarget.com

Methods of combating phishing

-- phishing.org

1. Keep informed about phishing techniques
2. Think before you click!
3. Install an anti-phishing toolbar
4. Verify a site's security
5. Check your online accounts regularly
6. Keep your browser up to date
7. Use firewalls
8. Be wary of pop-ups
9. Never give out personal information
10. Use anti-virus software

Methods of spotting phishing

-- techrepublic.org

1. Message contains a mismatched URL
2. URLs contain a misleading domain name
3. Message contains poor spelling and grammar
4. Message asks for personal information
5. Offer seems to good to be true
6. You didn’t initiate the action
7. You’re asked to send money to cover expenses
8. Message makes unrealistic threats
9. Message appears to be from a government agency
10. Something just doesn’t look right

Number one way of fighting Phishing at the GSC?

user education

GSC approach to user education

1. Newsletter submissions
   That are occasionally read

2. “Allstaff” talks
   Only about 350 people at the GSC, all of which fit nicely into an auditorium

3. Phishing campaigns

[anti] Phishing campaign

Gophish

Open source phishing framework (https://getgophish.com)

Windows servers
Individually crafted emails containing a suspicious link
Suspicious link is to an unknown external location
Can identify who clicked

Used to educate, not to punish or shame

Phishing campaign

From: BCGSCUsers@phsa.ca
Sent: Wed 12/20/2017 12:36 PM
To: Lance Bailey
Cc:
Subject: PHSA Cancer Agency Information System - UNAUTHORIZED ACCESS

Provincial Health Services Authority
Province-wide solutions. Better health.

Dear Lance Bailey,

You have received this email because you or someone had used your account from different locations. If you haven't recently tried to login to the PHSA network located at 177.143.23.170 (BR), someone else may be trying to access your account. You can view more info about this login attempt online.

If you suspect someone else may be attempting to access your account, please either:

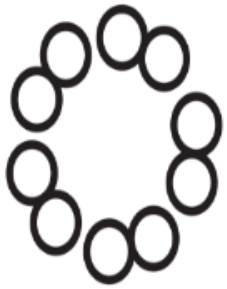
- Change your password immediately or
- Lock your account online and then request Systems assistance to regain access to your account.

Thanks for helping us maintain the security of your account.

The PHSA Support Team
phsasystems@phsa.ca

This is an automatically generated message. Unsubscribe

Phishing campaign



CANADA'S MICHAEL SMITH
GENOME
SCIENCES
CENTRE

What just happened?

This is an authorized phishing simulation conducted by GSC Systems. This simulation help us understand the effectiveness of security measures and improves the ability of staff to spot and correctly handle phishing emails.

Phishing is the name given to a type of scam, usually conducted via email, social networks, or instant messaging in which the attacker attempts to get the victim to click on a malicious link, open a file attachment, or trick the user into entering their password into a fake web site. Phishing emails often use offical logos, colours, and phone numbers in order to appear legitimate.

Please visit our wiki at https://www.bcgsc.ca/wiki/display/SysHelp/How+to+Recognize+the+Signs+of+Phishing+Emails for more resources on the dangers of phishing emails.

Please be more careful when clicking on links.

Phishing campaign

Results (Dec 2017):

- 342 emails sent out
- 82 people (24%) clicked the email
- 20 people (6%) clicked more than once
- 2 people (< 1%) clicked 5 times

Phishing campaign

Results (Dec 2017):

342 emails sent out
82 people (24%) clicked the email
20 people (6%) clicked more than once
2 people (< 1%) clicked 5 times

Yes, really, 5 times.

How to warm a security admin's cold cold heart

Message | WescanOutstanding.pdf (54 KB)

I got this email from a vendor, although I don't recognize the sender's name, and the attachment has a link inside it, which is unusual. Forwarding in case it's malware.

From: Tracy Fenton [mailto:tfenton@wescancal.com]
Sent: Wednesday, March 14, 2018 2:06 PM
To: Tracy Fenton
Subject: Tracy Wescan PAST DUE INVOICE

Thanks,

Regards,

Tracy Fenton

Admin. Asst./AP

Wescan calibration

Unit 9 - 12240 Horseshoe Way
Richmond, BC Canada V7A 4X9
Office: 604.275.0600 / 1.800.661.3177
Fax: 604.275.0610
tfenton@wescancal.com
www.wescancal.com

If you require a quote, please email **quotes@wescancal.com**

If you are looking to schedule your units for calibration, please email **scheduling@wescancal.com**

Royal Roads University

Don Devenney, CD GCWN GMON CIPP/C
IT Security Specialist
Royal Roads University

Background

Our phishing education program grew out of an account compromise that occurred in Nov. 2014

- Account compromised as a result of a phishing email sent to an Associate Faculty member
- Criminals used the Associate Faculty member's account to contact several students, many of whom subsequently had their accounts compromised.
- In all, we had 10 different SPAM email / compromised account incidents over the next 7 months as a result.

Something had to be done….

Initial Program

- Series of in-person presentations that:
  - Stressed job relevance
  - Stressed impact to organisation in real terms - time lost, cost, etc.
- Surveyed participants and adjusted presentations based on comments
- Reviewed presentations prior to presentation and updated as required.
- Focused on Staff / Faculty

Current State

- Program has matured

- Delivery is now an initial in-person knowledge transfer session, supported by repetition of key messages

- Repetition is achieved through:
  - SANS Securing The Human (STH) posters placed around campus
  - STH Phishing training emails.
  - Security Awareness website
  - Staff newsletter articles as necessary
  - STH program for National Cybersecurity Awareness Month

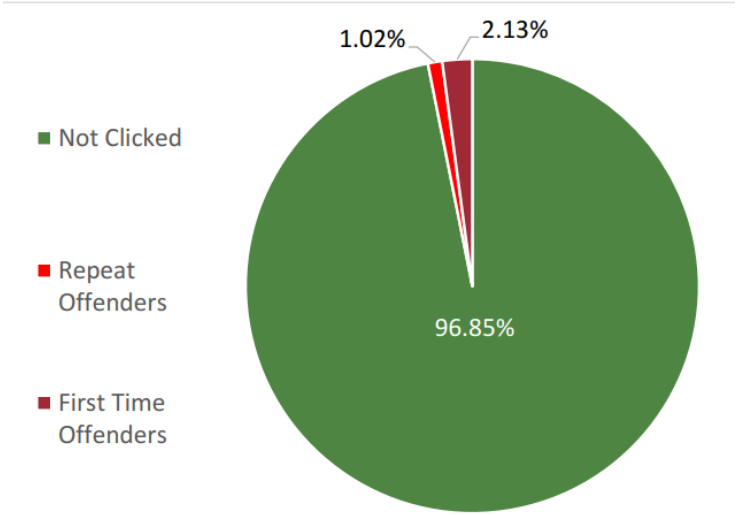
- In addition to the in-person sessions delivered to business units we also do abbreviated in-person sessions as part of the new staff on-boarding process.

We are also employing the CIRA DNS Firewall to (hopefully!) block connection attempts to C&C servers should someone open a phishing email that tries to "call home" to download a malicious payload.

Effectiveness

It’s all about the metrics….

- We haven't had a compromised network account or ransomware incident attributable to phishing since Feb 2017
- Using the SANS STH phishing program our "click" rate has been reduced to 3.15%



Program Strengths

- In-person delivery is highly effective, IF DONE RIGHT
- Repetition of the message through a variety of media enforces the initial training and keeps it fresh in the user's mind.
- We stress "you're not in trouble - talk to us“
- We reward success
- Staff like having an actual person they can contact. And they do...

Weaknesses

- In-person delivery can be difficult to achieve:
  - Requires specific skill set - NOT A JOB FOR A TECHIE.
  - Hard to scale.
  - Business Unit resistance to dedicating time for the training.
- Time
  - I'm a security department of one....
  - Keeping media resources updated and fresh.

Next Steps

- Develop an “Update on Cyber Security” presentation that we can take back to our original audiences.

- Create an on-line version of the “Update on Cyber Security” presentation that can be used as part of the on-boarding process for new Associate Faculty.

- Create a “Cyber Security Ambassador” program to:
  - Stimulate involvement of the various Faculty / Business units.
  - Create a sense of ‘ownership” around cyber security.
  - Lighten my workload (???)