The Phish Bowl
Managing the Phishing Frenzy at Brown University

Pat Falcon
Information Security Policy & Awareness Specialist

David Sherry
Chief Information Security Officer

March 31, 2015

This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution-NonCommercial-ShareAlike license, which grants usage to the general public with the stipulated criteria.
How to keep your head above water when it feels like you’re drowning in good intentions.
Goal

- Introduce you to a good model for creating your own “phishing central” with supporting procedures.
- Provide ideas for an awareness campaign to empower and engage your users in helping to thwart phishing attacks.
Overview

Context

- Computing at Brown
- Computing & Information Services
- The Information Security Group (ISG roles & relationships)
- The Phishing Frenzy of August 2013 (or, the Great Flood)
Overview

The Phish Bowl

- What it is (and isn’t)
- Process: creation, roll-out, results, next steps
- Tour ([brown.edu/go/phishbowl](brown.edu/go/phishbowl))
Your Phishing Story

- A chance to share your solutions
- What have you built?
- Or perhaps, rebuilt?
- Inspired by this talk?
Sound like a plan?
Sound like a plan?
Computing at Brown (the numbers)

- Faculty: 718 (if adjunct, visiting, clinical, and other "non-regular" faculty included 2,000+)
- Staff: 3,207 (includes exempt, non-exempt, limited duration, union and bio-med)
- Students: 8,848 (6,264 undergrads, 2,094 graduate and 490 medical students)
- Hospital affiliation: 3,508 (includes affiliated but not on payroll)
- Total number of accounts: ~ 20,000 + alumni + applicants

» All possible phishing victims!
Computing & Information Services (CIS)

- Large, mostly centralized computing organization
- Over 200 full-time staff plus student employees
- Departmental IT groups (including Advancement, BioMed, Center for Computation & Visualization, Division of Campus Life & Student Services, Facilities Management and University Library)
- CIO reports to Provost, eight direct reports
- http://it.brown.edu (new website)
Information Security Group (ISG)

- Small team of two works closely with allies to extend its impact
  Network security engineers (separate group), IT Service Desk, decentralized computing support (DCCs)

- CISO – CIS senior director, consulted on all major IT projects
  OGC, Internal Audit, VP Research, Bio Med IT director (HIPAA), CCV, Asst VP of Business & Finance / Commerce Committee (PCI), DPCRM / Univ Library, Alumni Relations, etc.; in position since 2008

- Policy & Awareness Specialist
  Responsible for National Cyber Security Awareness Month and Data Privacy Month events; all communication including website, alerts, social media and marketing; in position since formed in 2004
Phishing Frenzy

And then the dam burst in August 2013 and it soon felt like we were gasping for air (42 compromised accounts just on Aug 1 & 2!)
Along the phishing perimeter
Winter of 2014
Hope all is well with you, am out of town I travel to Turkey for a short vacation, I have a little problem here my ATM card didn't work here...
I tried about 5 different ATM booths no money was dispensed.
am stranded here I don't have any money with me. I need you to wire me 2000 Euro or whatever amount if not all via western Union I'll refund back your money immediately I get back next week.
Let me know if you can help me out. Hope to hear from you soon.

Thanks,

Sentha
Learn how to spot phishing attempts.

Look for them in the Phish Bowl ( brown.edu/go/phishbowl ).

Report sightings to phishbowl@brown.edu.

Make phishing *History*!

This message brought to you by the *Information Security Group, CIS*
The Phish Bowl (an origin story)

The Idea

- Began as a suggestion to segregate phishing alerts – provided by the Brown community – on one basic page
- Envisioned as a moderated online upload site
- Would be used to feed social media (“Phish Feed”)
The Phish Bowl (an evolution)

But it could also be an opportunity to develop a more timely and efficient system for managing phishing threats to better protect the Brown community.

- do this by standardizing incident response
- address general confusion (community and IT staff)
- expedite alerts to prevent escalation of phishing incidents
The Phish Bowl (an evolution)

But it could also be an opportunity to:

- raise awareness and be a teaching tool.
- be the focus of our back-to-school campaign and National Cyber Security Awareness Month efforts in October.
- empower the community by appealing to their nature to serve.
The Phish Bowl (an evolution)

In other words . . .

it became *less about technology*
and more about marketing and social engineering (the good kind).

The Phish Bowl (an evolution)

In other words . . . it became less about technology.
The Phish Bowl (an evolution)

and more about marketing and social engineering (the good kind).
The Phish Bowl (an evolution)

In other words . . . it became less about technology and more about marketing and social engineering (the good kind).
The Phish Bowl (the process)

- Creation & tour
- Roll-out & marketing materials
- Results
- Next steps
The Phish Bowl (creation)

Timeline:
- March & April 2014: “Phish Feed”; proposal written & finalized
- May: Approval by senior directors to proceed
- June & July: Meeting with web team (design* & marketing plans)
- August: Website in place; messages firmed up (announcements, canned response); workflow document created; training; release

* Design and name inspired by Cornell’s “Phish Bowl” (thanks!)
To automate or not to automate?

- Web form + dashboard for a moderator
- Could auto-strip URLs *but* how to handle Brown names or other content not to post?

**Bottom Line:**
How to make it as easy as possible for user?
Just forward it!
The Phish Bowl (tour)

brown.edu/go/phishbowl
The Phish Bowl (roll-out)

- 8/15 (2014): IT Service Desk demo and training
- 8/18: “Go Live!” date
- 8/19: Targeted email (CIS, department computing coordinators)
- 8/25: Morning Mail (morningmail.brown.edu)
- 8/29-30: Back-to-School
- 10/1-31: National Cyber Security Awareness Month
- 10/29: Brown’s Safety Resource Fair (every October)
Bowl, Phish <phishbowl+canned.response@brown.edu>
to me |

Thank you for alerting us to the suspicious email.

Are you wondering if what you received is phishing?
Please check the Phish Bowl at brown.edu/go/phishbowl to see if it or a similar email has already been reported. If it hasn’t, then should we determine that it is phishing, we will add it to the Phish Bowl.

Did you receive a phishing email and want to know what to do with it?
If you are sure it is phishing and opened an attachment or clicked a link, then we recommend that you report it as phishing to the Gmail team (from within the message, click on the down arrow to the right of the REPLY button and select "Report phishing"). And as above, if the message you forwarded is not already in the Phish Bowl, we will add it.

Did you accidentally click on a link, fill in a form or open a document?
If you did respond to the email in some way, then your account or personal information could be compromised. Please follow the instructions below as soon as possible. Once you have completed all the listed steps, notify the IT Service Center (help@brown.edu) to let them know that your account is once again secure.

Thank you again for reporting this issue.

Please note: This account is actively monitored during regular business hours and periodically at other times.

Pholks @ the Phish Bowl | Computing & Information Services
Instructions for Recovering a Compromised Account

1. PASSWORDS: If you HAVE responded to the phishing scam, please change your Google password immediately at [www.brown.edu](http://www.brown.edu) > [myaccount](http://myaccount) (under the subheading “Change Google Apps@Brown Password”). If your Brown password is the same, change it as well. That goes for any other accounts that might have had the same password. (Note that you should not be using the same password for non-Brown accounts.)

2. OTHER SESSIONS: Log into your Brown Gmail account, using your new password (make sure to uncheck the “Stay signed in” box). Check the account activity (bottom of [Inbox](http://gmail.com), right side) by clicking on [Details](http://details). Then in the new window, “[Sign out all other sessions](http://sign-out)”. (This will force all computers that have your Gmail account open to sign out and prevent an attacker from continuing to use your account if currently logged in.)

3. SENT FOLDER: Check your [Sent Mail](http://sent) folder to see if anything suspicious has been sent from it. If so, this is a definite clue that your account has been compromised.

4. SUSPICIOUS ACCOUNTS: Check your [Google Account settings](http://settings) and remove any suspicious accounts (Settings > Accounts > Send Mail As). While in Settings, you should also check your [Filters and Forwarding](http://filters) to make sure there have not been any unwanted changes (e.g. all of your email is being forwarded to someone else’s address).

5. GOOGLE DRIVE: As an extra precaution, check your [Google Drive](http://drive) for any files that were created to collect others’ information. Please check the [Trash](http://trash) folder as well as files could be hidden here. Report any findings to [isc@brown.edu](mailto:isc@brown.edu).

6. SCAN: Run a [scan](http://scan) of your system to check for any viruses or other malware. Brown has anti-malware programs available for download and use at [brown.edu/go/software](http://brown.edu/go/software).

QUESTIONS or NEED HELP? Please contact the Brown IT Service Center at [401-863-4357](tel:401-863-4357).

The Information Security Group reminds you to never provide your ID, password, or personal information via email. Computing and Information Services at Brown, as well as all legitimate businesses and services, will never request your personal information or credentials via email.

More information on phishing can be found at [http://www.brown.edu/go/phishing](http://www.brown.edu/go/phishing) and in Google’s document [Messages asking for personal information](http://www.brown.edu).
Introducing the 'Phish Bowl'

Date: Monday, August 25, 2014
From: The Information Security Group, CIS <ISG@brown.edu>
To: All Faculty, All Staff

Phishing continues to plague everyone, with no end in sight. While we can't make it go away, the new Phish Bowl should make it easier to deal with.

The Phish Bowl was created as the one spot to check for phish. If you spot or are unsure about one, just check the Phish Bowl. If it's there, no need to report it. If not, forward it to PhishBowl@brown.edu. It will be added so others are aware of it.

Visit http://www.brown.edu/go/phishbowl to see the latest alerts and to learn more about phishing.
The Phish Bowl (announcement)

The Phish Bowl means no need to send a suspicious email to the IT Service Desk, ISG, DCC, a supervisor, colleague or someone else. The only place to report it, if not already in the Phish Bowl, is to forward it to PhishBowl@brown.edu. It’s that simple.

It’s not that we haven’t been happy to have had SO many reports of phishing. This has demonstrated a growing awareness of phishing within the Brown community. But it hasn’t always been the most effective way to get the word out or deal with phishing. The Phish Bowl should save confusion and redundant notifications, and let us focus on dealing with phishing outbreaks and their impact.

By simplifying the process -- one place to check, and one email address to contact -- everyone’s life should be a little less confusing, a bit easier. And safer.

One other change. We will be more proactive in dealing with compromised accounts. If your account has been hacked, we will try to reach you by phone, but if we can’t do so in a timely fashion, to protect your account from further abuse and the accounts of others, we will need to temporarily lock it. You will then need to contact the IT Service Center (help@brown.edu or 863-4357) to reactivate it.

To learn more about what phishing is and how to avoid it, visit http://brown.edu/go/phishing.

Notes:
1. We attempt to reach victims by phone rather than email because the hacker already has control of your account and on occasion has used emails sent to compromised accounts in new phishing emails.
2. The procedure varies slightly for faculty, who may be harder to reach (a faculty account will remain open for two business days before suspension).
The Phish Bowl (marketing)

Back-to-School

SPOT the PHISH brown.edu/go/phishbowl
STOP the PHISH phishbowl@brown.edu
The Phish Bowl (marketing)

October / National Cyber Security Awareness Month

- Website (links to events and online contest)
- Ads in student newspaper (Brown Daily Herald)
The Phish Bowl (marketing)

This October

SPOT the Phish 2
STOP the Phish

& maybe win an iPad mini, too.

October is National Cyber Security Awareness Month, a time to tweak your computing safety skills to protect yourself and others. The focus this year is on phishing.

Let’s face it. Phishing is not going away, it will probably get better (i.e., scammers get cleverer) as well as worse (heavier and more frequent attacks). As a result, you or someone you care about could be the next phishing victim.

What to do? Make it safer for everyone by learning to SPOT the Phish 2 STOP the Phish. Enter our weekly quizzes to test your phishing knowledge AND collect chances toward our drawing on 10/31 on an iPad mini, Nexus 7 and more prizes.

Plus, there are lots of ways to connect with us (and collect more chances on the drawing): stop by our table at Brown’s Safety Resource Fair (10/8), attend our Brown Bags (10/9 & 10/23), and come to the screening of CODE 2600 (10/15). Details at brown.edu/go/SpotThePhish.

National Cyber Security Awareness Month :: Oct 2014 presented by the Information Security Group, CIS ISG
National Cyber Security Awareness Month
National Cyber Security Awareness Month
National Cyber Security Awareness Month

The Phish Bowl
National Cyber Security Awareness Month

Catch the Phish & win a prize!

Play our game for a chance to win a prize. Drawing at 2:00 PM; you're also entered in the 10/13 raffle for an iPad mini, Nexus 7, & more!

Finished at the Cybersecurity Center 11/04/13

The Phish Bowl

BROWN
The Phish Bowl (the results)

In the crucible / trial by fire
- The timing couldn’t have been any better

On the whole, it worked as intended
- On 8/25 – 8/26, we received 55 reports to phishbowl
- During that same period, personal account (5), ISG (9), and has continued to diminish over time

Hits on brown.edu/go/phishbowl
- Still get reports for alerts in Phish Bowl, but it is consulted
The Phish Bowl (the results)
The numbers:

- 1,160+ emails sent to phishbowl@brown.edu since 8/25
  (from 575 unique senders)

- 160+ alerts in the Phish Bowl since 8/25

- 207 compromised accounts since 8/25

- 171 compromised accounts between 8/1/2013 & 8/25/2014
  (42 on 8/1 & 8/2 IRS.gov)
The Phish Bowl (lessons learned)

#1: Can’t bring in the robots just yet
- even with auto-response, still need the human-touch to edit & respond at times

#2: Handling content
- spam, legitimate email, duplicates, vishing, screen shots

#3: A chance to break out the markers & whiteboard
- teachable moments + opportunity for more connections w/ community

#4: Make the message even simpler and/or re-educate
- phishbowl@brown.edu worked; brown.edu/go/phishbowl not as well

#5: Hardest thing: the stories of victims
#1: Survey (general community + IT Service Desk)
- name recognition, what worked or didn’t, suggestions

#2: Fire up phase 2 of marketing plan
- monthly reminders + quizzes; set timeframe

#3: Review phishing alerts
- archive, rebundle, delete
Your turn – what’s your story?
Who handles phishing at your school?
Is there a formal set of procedures or standard practice?

How is the community notified of major outbreaks?
What is the community’s role (active, passive, none)?

Do you have anything like the Phish Bowl or plans to create it?
Along the phishing perimeter, 
The beginning of 2015
DOCUMENTS FOR YOU
Compliment of the season !!
I need you to go through this uploaded files. Due to the size I have zipped and compressed it making it accessible via google secure folders.
For immediate access click **Access Files Here** just sign in with your email, This files are very important.

Let me know what you think.
Regards,
Kristin Bishop, Asst. Professor
Learn how to spot phishing attempts.

Look for them in the Phish Bowl (brow.edu/go/phishbowl).

Report sightings to phishbowl@brown.edu.

Make phishing History!

This message brought to you by the Information Security Group, CIS
Resources

- brown.edu/go/phishbowl  (Cornell’s Phish Bowl: www.it.cornell.edu/security/phishbowl.cfm)
- http://it.brown.edu (CIS home page)
- Spot, Protect and Recover from Phishing
  www.brown.edu/information-technology/knowledge-base/article/1248
- Anti-Phishing Working Group (www.antiphishing.org/)
- Higher Education Information Security Council (HEISC)
  www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative
- Awareness and Training (A&T) Working Group
  www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/community-engagement?
Thank you for attention.

Pat Falcon: pat_falcon@brown.edu
Information Security Policy & Awareness Specialist

David Sherry: david_sherry@brown.edu
Chief Information Security Officer

The Information Security Group:
isg@brown.edu | brown.edu/go/isg

Reminder from program committee to fill out your session evaluation.