What is phishing?

According to the Anti-Phishing Working Group (APWG):

"Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit web sites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond.

Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning."

How to spot a phish

A good place to start is by visiting the Phish Bowl for a wide variety of examples (brown.edu/go/phishbowl). Some of the commonalities you'll find there provide contain one of more of the following traits of a phony and possibly dangerous message:
The TO field is blank or for another person.
It contains an urgent request for personal information.
It includes grammatical errors or typos.
The message is threatening (Do X right now or lose Y).
It has a link (or submit button), probably to an unsecured address (NOT https).
When you hover over the link, it directs you to an address (usually suspicious) other than what is displayed.
The message has an attachment.

How to protect yourself
The simplest 1-2-3 advice is: (1). Be wary (2.) Stay vigilant (3.) Use common sense.

Most importantly, use two-step verification on your Google email account for an extra layer of protection.

For a few other specifics on what you can do, follow this APWG list of tips to prevent being hooked by a phishing attempt:

- Be suspicious of any email with urgent requests for personal financial information.
- Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don't know the sender or user's handle. Do use the "hover to discover" technique to see if the URL directs you to a suspicious address. For smart devices "don't get sold; press and hold", described in Reveal the True URL of a Link.
- Avoid filling out forms in email messages that ask for personal financial information.
- Always ensure that you're using a secure web site when submitting credit card or other sensitive information via your Web browser.
• Remember not all scam sites will try to show the "https://" and/or the security lock. Get in the habit of looking at the address line, too. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?" Be aware of where you are going.
• Consider installing a web browser tool bar to help protect you from known fraudulent web sites. These toolbars match where you are going with lists of known phisher web sites and will alert you.
• Regularly log into your online accounts and check your bank, credit and debit card statements to ensure that all transactions are legitimate.
• Ensure that your browser is up to date and security patches applied.

What to do when you spot a phish

• If you receive a suspicious email and you're not sure if it's a phish, check to see if it's in the Phish Bowl (visit it at brown.edu/go/phishbowl).
• If it's not in the Phish Bowl, forward the email to PhishBowl@brown.edu so that it can be added.
• Alert Google if you do receive a phish (from within the message, click on the stack of three dots to the right of the REPLY button and select "Report phishing"). This will send that message immediately to the Gmail Team for analysis and filtering.

What if the phishing attempt arrives by phone (called vishing, for "voice phishing")? We recommend that you ask the caller to leave a name and number to reach them at later (say that you will call back at a more convenient time, after verifying with department head that you should be taking the call). While on the phone, try to collect the following information and then forward these details (and any others you might have) to phishbowl@brown.edu:

• Affiliation of the caller (do they say they are internal to Brown? External? A vendor?)
• Name used by the caller
• The information they were seeking
• The number called from (this could be number displayed in Caller ID, the number they said to call if you had questions and wanted to get back to them, or both)
• Anything distinguishing about the voice (gender, accent, age, etc.)
• Time of day the call was received

Compromised?
If you think you might be the victim of a phish (or other suspicious email) or are concerned your account may have been compromised, you should take immediate action and complete the following recommendations:

1. Change both your Brown and Google passwords (www.brown.edu/myaccount).
   If you used the same passwords for other accounts, you should change them as well.
2. Check the account activity at the bottom of your Inbox, and sign out of all other
sessions if found.

3. **Check your Sent Mail** folder to see if anything suspicious has been sent from it, which would confirm that your account has been compromised and let you know who would have received email from your account.

4. **Disable unwanted email forwarding** that may have occurred when the account was compromised. (Settings > Forwarding and POP/IMAP > Disable forwarding)

5. **Run a scan** of your system to check for any malware.

6. **Check your Google email settings** and remove any suspicious accounts. (Go to Settings > Accounts > Send Mail As)

7. **Check your Google drive** for any suspicious files you might find there, especially ones that were created to collect others' information (**check your Trash folder as they are often hidden here**). If you do find any, report this to ISG@brown.edu.

8. **Protect your Gmail password** and enable two-step verification for your Google email account if you have not done so already.

If you need assistance, contact the IT Service Center. And should confidential or sensitive information resides on your computer or on your Google Drive and may have been compromised, please report this to ISG@brown.edu.

What to do if you become a victim of identity theft

Unfortunately, there is no way for us to track down the scammer. These criminals use fake addresses and relay points around the globe, and usually shut down the servers and addresses in less than 24 hours, while moving on to a new one. Major investigations by the FBI on issues like this take years, and oftentimes have no results. There are some things you can do. You can start by following the same five steps in the previous section. In addition to those, you should:

- Review the Federal Trade Commission site (ftc.gov) for tips, to file a complaint, and/or log an identity theft concern. See their Privacy & Identity page for tips on identity theft repair, credit freezes, and much more.
- Contact the Attorney General Office from the state you reside and log a complaint.
- Contact the three credit bureaus and place a fraud alert on your SSN (Experian, TransUnion, and Equifax); ask for free credit reports to set as a baseline. Read Recover From Identity Theft for details.
- **Note: According to the Social Security Administration, if you have become a victim of identity theft and "you have done all you can to fix the problems resulting from misuse of your Social Security number and someone still is using it, we may assign you a new number." See their FAQ for details.**

Sharpen and test your skills

There are several excellent tutorials to help you spot phishing attempts and learn how to avoid them, and quizzes to test your awareness of various phishing tactics. You may wish to check out one or more of the following listed here.
Tips, tutorials & videos

- How to Spot Phishing Scams (video from Howcast)
- Phishing Scams: Avoid the Bait (source: OnGuardOnline.gov)
- Phishing: Don't Take the Bait (Federal Trade Commission)
- OnGuardOnline.gov Phishing page (for more examples of phishing messages)

Phish Bowl + CIS notifications

CIS will post phishing alerts to the Phish Bowl, which also appears on the IT at Brown home page. In addition, more widespread outbreaks will be announced in Today at Brown.

Tags

Security