BROWN

Spot, Protect Yourself, and Recover from Phishing

Stephanie Obodda - 2025-01-21 - Comments (0) - Phishing

Jump to:

What is phishing?

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

"Phishing is a crime employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

Social engineering schemes prey on unwary victims by fooling them into believing they are dealing with a trusted, legitimate party, such as by using deceptive email addresses and email messages. These are designed to lead consumers to counterfeit Web sites that trick recipients into divulging financial data such as usernames and passwords.

Technical subterfuge schemes plant malware onto computers to steal credentials directly, often using systems that intercept consumers' account usernames and passwords or misdirect consumers to counterfeit Web sites."

Phishing communications can arrive in an email, text, phone call or even during an in-person solicitation, so it is important to learn the common warning signs.

How to spot a phish

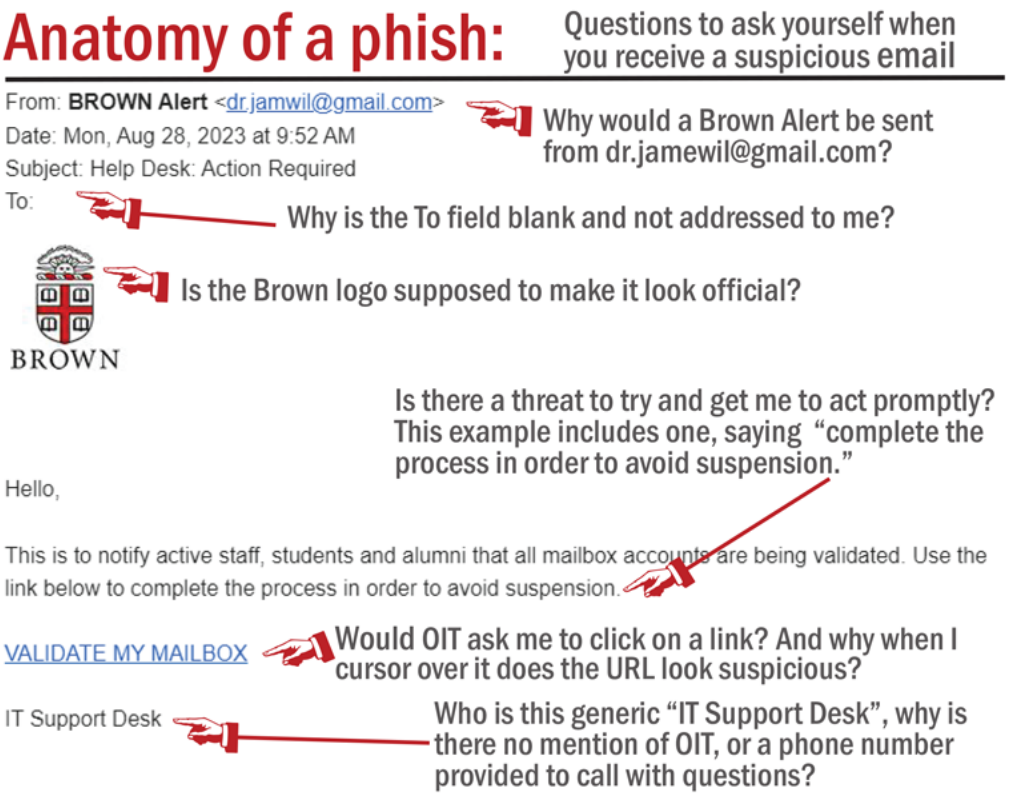
Detecting a phish is often a matter of feeling that something is "off" and not quite what it seems, because most phishing attempts are emotional button-pushers. They might appeal to *fear* (do X or Y will happen), *greed* (you're a lucky winner of $$$), *curiosity* (a file called Salaries.xlxs has been shared with you), or perhaps to one's *sense of self and duty* (a superior has an immediate need for your assistance).

When reading email, here are some traits of a phony and possibly dangerous message that

you should be aware of and report:

- The TO field is blank or for another person.
- The email name and address of the SENDER don't match (name is familiar but address is not). These are often called "impersonator" or "spoofing" emails.
- The sender says they are from Brown but doesn't use their @brown.edu address.
- It contains an urgent request for an action or information.
- It includes grammatical errors or typos.
- It has an offer that seems too good to be true (like a job offer for $400/week for little work and no experience)
- 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.

Visit the **Phish Bowl** at **brown.edu/go/phishbowl** for a wide variety of examples of some of these tell-tale signs of phishing.



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

Here are some tips to prevent being hooked by a phishing attempt:

- **Not so fast!** 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.**
- **Confirm the actual sender.** While it is easy to impersonate other accounts to look like they are coming from a reliable source, it's also simple to check for the actual sender. Follow the details in the Google help article **Trace an email with its full headers.**
- **Avoid filling out forms in email messages** that ask for personal financial information.
- **Check your email account activity for anything that isn't familiar.** You do this from your Inbox by scrolling down to "Last account activity" in the bottom right and clicking on "Details". The resulting chart displays the method of access (such as browser or mobile device), location, and when this occurred. You can also launch a Security Checkup from this page. The Google article **Last account activity** provides more details on what you can do.
- **Always use a secure web site** when submitting credit card or other sensitive information via your Web browser.
- **Check the address line.** Remember not all scam sites will try to show the "https://" and/or the security lock. 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.
- **Block or unsubscribe from inappropriate or harassing emails.** You can also **Create rules to filter your emails**. If you have experienced harassment, depending on the type, you may want to report the incident at **reportbias@brown.edu** (more details on the Office of Institutional Equity and Diversity's **Incident Reporting page**).
- 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 you think may be phishing, **report it to OIT using the Phish Alert button**.
- Visit the **Phish Bowl** to see if the message has been reported by other members of the community.

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 where they can be reached later (you could say that you "you will call back at a more convenient time, after verifying with a 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, or a vendor?)
- Name used by the caller
- The information they are 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.)
- When the call was received

Compromised?
If you think you might be the victim of a phish or are concerned your account may have been compromised, you should take immediate action and complete the following recommendations outlined in **Secure a Compromised Gmail Account**. Once you've attempted to secure your account, **report the incident to OIT.**

If you believe **confidential or sensitive information** residing on your computer or Google Drive may have been compromised, please additionally report this directly to ISG@brown.edu.

If you additional questions or security concerns, do not hesitate to contact the **IT Service Center**.

What to do if you become a victim of a scam or 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 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.
  > Read **What To Do If You Were Scammed** for advice if you paid a scammer, gave one your personal information, or if a scammer has access to your computer or phone.
  > Go to **ReportFraud.ftc.gov** to report and fight fraud.
  > Learn more about **identity theft**, also on the FTC's site. If you think someone is

using your personal information to open accounts, file taxes, or make purchases, visit **IdentityTheft.gov** to report and recover from identity theft.

- 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.**

Tips from the Federal Trade Commission (FTC)

- **Avoiding and Reporting Phishing Scams**
- **How Scammers Tell You To Pay** (video)
- **How to Recognize and Avoid Phishing Scams**
- **Phishing: Don't Take the Bait**

Phish Bowl & Phishing notifications

Phishing alerts are posted to the **Phish Bowl,** with more widespread outbreaks announced in **Today at Brown**.