How To Recognize and Protect Yourself Against Email and Social Network Phishing

by Brannon Cullum

Phishing is a way of attempting to acquire sensitive personal information such as usernames, passwords and financial information by imitating a trustworthy source in an electronic communication. It most commonly happens via email or instant messaging.

Most incidents of phishing involve using some type of technical deception (like a link) to direct a user to a site that looks and feels like the legitimate site belonging to the organization behind the email, but is actually a fraud. A lot of web browsers now have anti-phishing software built in, meaning that if you go to a site that it deems suspicious and cannot validate its security certificate, it will warn you before you can proceed to the actual site warning you that the site might be malicious. However, phishing scams have grown quite sophisticated and can be difficult to detect.

During the uprising in Tunisia, a number Facebook users inside the country discovered that their accounts were being phished by the government. According to reports, the Tunisian Internet Agency was modifying web pages by injecting them with JavaScript to steal usernames and passwords on popular sites like Google, Yahoo, and Facebook. People logging onto the sites unknowingly had their sensitive log-in information stolen. The government then quickly moved to delete Facebook accounts and groups.

With many governments stepping up their game and becoming savvier in their attempts to monitor and track dissidents online, it's important to be aware of the signs of phishing and what you can do to better protect your online accounts.

Share

Step 1.

If you receive **an email that looks suspicious**, there are a number of signs that it may be a phishing email, including:

- It usually comes from an institution or company you are likely to already be familiar with or trust, like a bank, government agency, or social networking site.

- The **greeting is usually generic** and doesn't address you personally. It may open with "Dear Customer" or "Dear [Name of company] User" rather than your first name or username.

- The email may contain **official-looking company logos and/or signatures**.

- The email **asks you to verify account information** like your username, password, or other personal information (date of birth, Social Security number, address) by sending an email or clicking on a link. It may sound something like this: *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*

- The email contains a link that, upon first glance, look like a valid link. However, if you hover over the link with your mouse to see the actual URL address, you can tell if it is the same link or something else. Look for any misspellings in the URL.

- You are asked to call a phone number and provide personal account information.

- There is a **sense of urgency** in the message such as: "Your account may be deleted if you do not respond in 48 hours."

Step 2.

If you believe the email you have received is a phishing attempt, there are a number of immediate steps you can take:

- Don't **reply** to the email.

- Don't download and open any **attachments**.

- Don't click on any **links** in the email. Instead, call the company or log onto the website directly by the web address in your browser.

- **Never send sensitive personal information** like passwords, credit card information, or detailed personal information (date of birth, Social Security number, address) via email.

- **Contact the institution or company** via their support page and alert them to the potentially deceptive email. Forward the questionable email and/or take a screenshot of the page. If you forward an email, include the entire original email including the subject line and header information. Report the email to the company via their support or security contact.

Step 3.

Take the necessary steps to protect yourself against phishing in the future.

- **Use HTTPS** to access your webmail. (It's now default on many services like Gmail).

- It's always a good idea to **update your passwords** as well. Learn how to create strong passwords and passphrases here.

- Make sure you have **updated your browser software**. Most browsers warn you if a link you are opening could potentially be malicious because they have anti-phishing software integrated

into the software. It's important to have the most up-to-date version of your browser with the latest security patches

- Make sure to **use different login names and passwords** for each of the websites you use.

- If you used Google Gmail, check out our how to guide for using the webmail service more securely.

Step 4.

As social networks have grown in popularity, the number of phishing attempts on sites like Facebook has skyrocketed. **What does Facebook phishing look like?**

- **Check the URL of the Facebook page**. Always log onto Facebook via a legitimate domain https://www.facebook.com. Don't log into Facebook if it is a similar but different domain. A fraudulent website may include the term Facebook before the domain (.com). This is called a subdomain. For instance, the address facebook.com.profile.a340ah3.com looks legitimate, but if you look more closely, the domain is actually a340ah3.com not facebook.com

- Be suspicious of any link, message, wall posting, or pop-up window that requires an additional login or asks you for your personal account information. Remember, **a phishing attempt could come from one of your Facebook friends** whose account has been compromised.

Step 5.

If you believe your account is being phished or you receive a suspicious link, message, post, or pop-up window that you believe is phishing:

- **Report** it to Facebook by sending an email to privacy@facebook.com. Visit the Facebook Help Center to get more specific help regarding your account.

- **Don't click on any links** in the post or message.

- **Never send sensitive personal information** like passwords, credit card information, or detailed personal information via a Facebook message.

- **Change your password** immediately. Learn how to create strong passwords and passphrases here.

- If the message or post comes from a Facebook friend, immediately **contact that person** to let them know that their account has been compromised. The same goes for a message or post coming from a company or oraganization you follow on Facebook.

- Share this knowledge with your friends!

Step 6.

Take the necessary steps to protect yourself against Facebook phishing in the future:

- **Enable HTTPS for Facebook.** In the case of Tunisia, experts found that the embedded JavaScript only appears when Facebook was accessed with HTTP instead of HTTPS, underscoring the importance of using HTTPS whenever you log into social networking sites.

- Always make sure you are logging onto Facebook via a legitimate domain.

Step 7.

- If you have given out your personal information and believe you've been the victim of phishing, check out the Anti-Phishing Working Group's advice on what to do.