**Phishing**

**In this article, you will learn about how attackers use psychology to bypass technical security measures.**

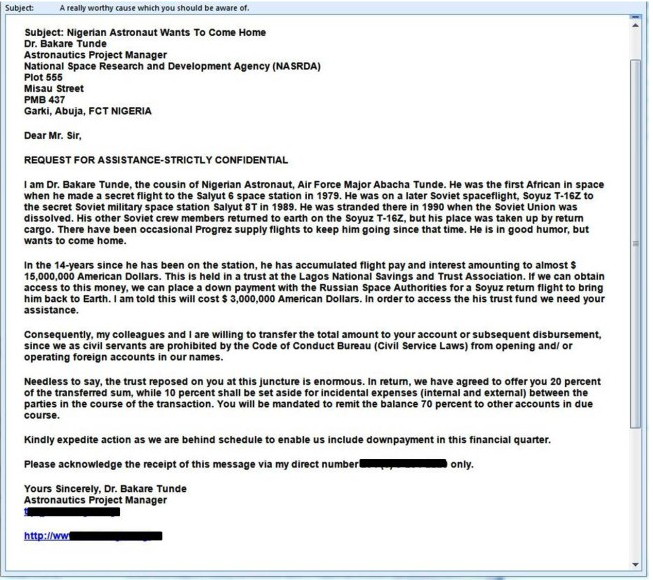
*Note: Attempting to phish the credentials of someone without their express consent is illegal. The information presented in this course in no way encourages or condones phishing, and should not be used to attempt a phishing attack.*

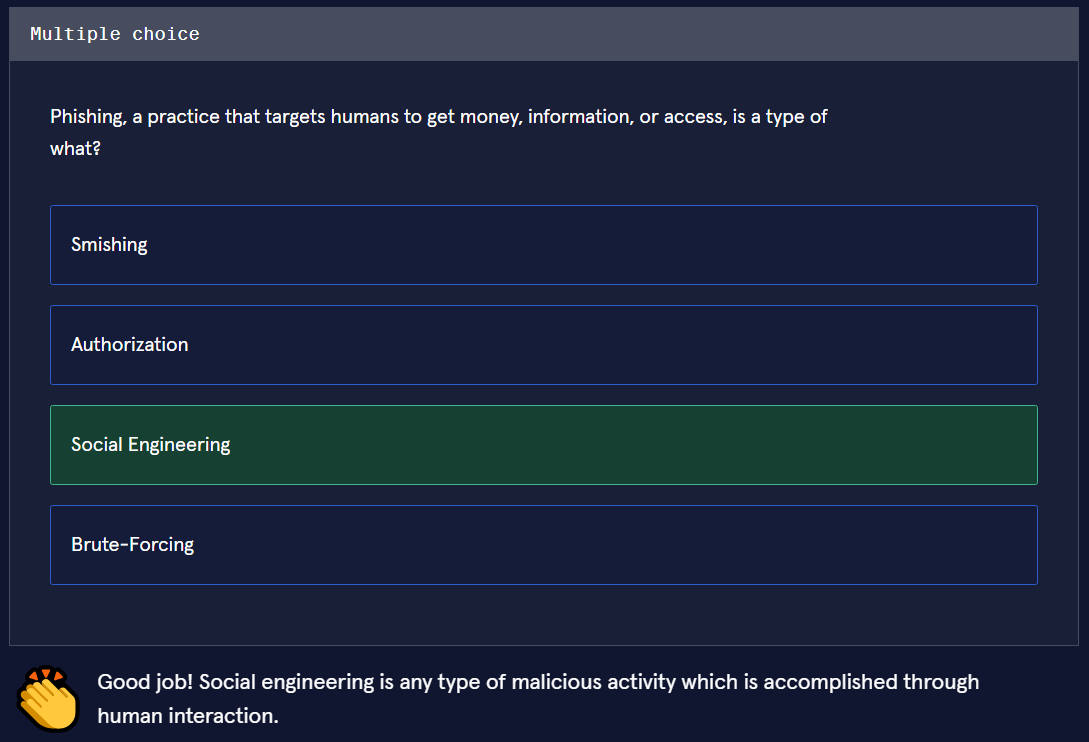
Phishing is one of the most well-known types of cyber attacks. The average internet user has never heard of Kali Linux or written Python scripts to guess passwords, but everyone knows not to respond to an email from a down on their luck Nigerian Prince (well, [almost everyone](https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html)).

One of the reasons that phishing is so common is because it works! No matter what technical controls are in place to secure a system, humans within the system are still hackable. The practice of tricking humans to get important data or access is also known as **social engineering**.

Estimates range on how effective phishing is, but given that it can be used for everything from credential theft to loading malware in systems, Verizon labeled it [the biggest threat to small organizations in 2020](https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-go-round).

Sometimes phishing attacks can seem comically implausible, such as this [phishing email from an unfortunate astronaut lost in space](https://www.anorak.co.uk/428124/money/nigerian-astronaut-lost-in-space-needs-3m-to-get-home-could-be-a-scam.html) below. However, with phishing attacks becoming both more common and more sophisticated, it’s vital to be able to identify and stop phishing attacks.





## Different Types of Phishing

All types of phishing rely on social engineering to get a victim to take some action, but there are different methods and targets beyond email, for example:

* [Vishing](https://us.norton.com/internetsecurity-online-scams-vishing.html) (from “voice phishing”), which refers to the spam calls in which an attacker claims to be from a victim’s bank or law enforcement and tries to extract information.
* [Smishing](https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html) (from “SMS phishing”) is when an attacker attempts to do the same thing over text message, by sending a malicious link.
* Webpages, which we’ll discuss in this article.

Phishing is also categorized by who it targets. Many phishing campaigns send out mass spam emails to individuals and organizations, hoping to catch a victim in a wide net. But sometimes, an attacker has a specific target in mind and sends that target a dedicated, personalized email. This is known as [spear phishing](https://www.csoonline.com/article/3334617/what-is-spear-phishing-why-targeted-email-attacks-are-so-difficult-to-stop.html). If the target is extremely sought after, like the CEO of a company, it is known as [whaling](https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack).

Whether it is used to trick someone into sending money, to harvest login credentials, or to download malware, phishing targets humans as an initial attack vector.

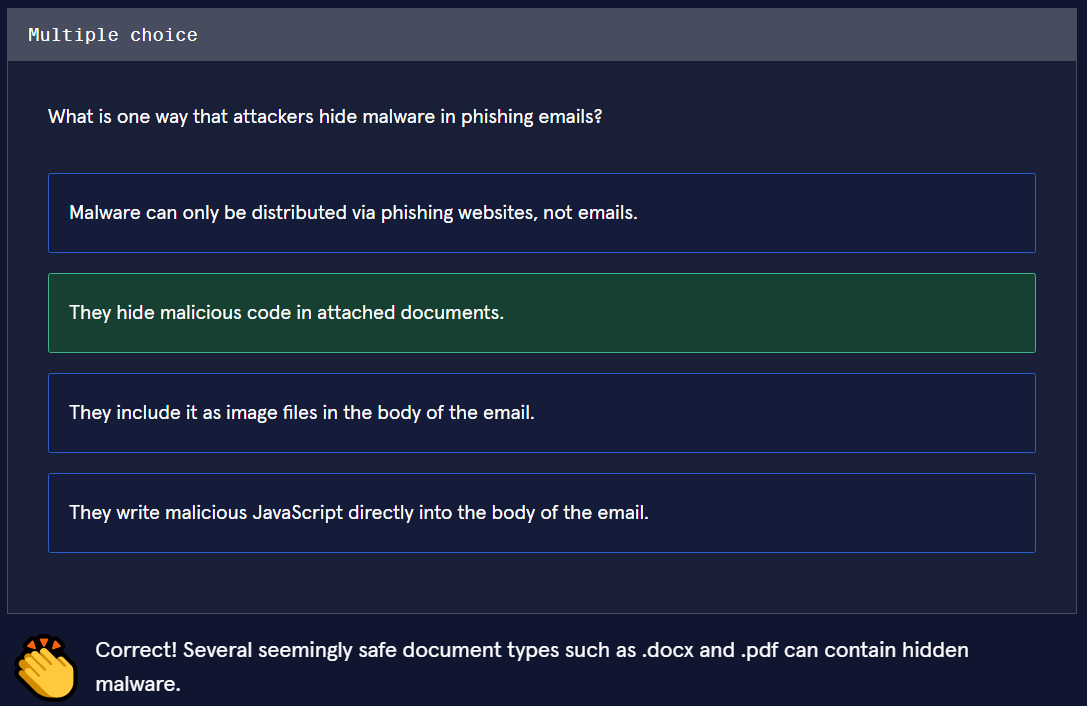


## How Does Phishing Work?

Sometimes phishing attacks are just emails or phone calls that attempt to get a victim to send an attacker money or payment information. Others, such as those that get people to click on links that download malware onto their systems, require more technical finesse. For example, an attacker could:

1. Embed a PDF or Word document with malicious code.
2. Attach it to a phishing email.
3. Social engineer a user into downloading and opening it, executing the malicious code.

Often, this malicious code contains the functionality to further spread the virus by sending more phishing emails to the user’s contacts.

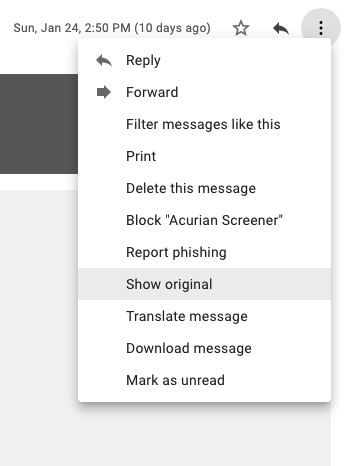


### Email Spoofing

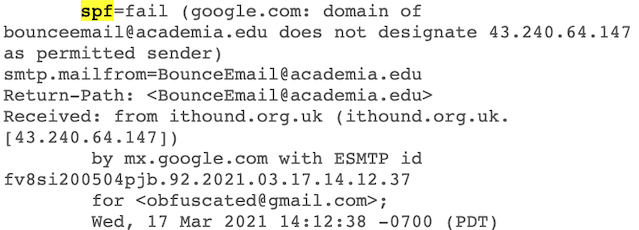
Email spoofing refers to when an attacker falsifies their email headers to make it appear as though the email is coming from someone else. Spoofing is a common component in phishing emails, used in as many as [90% of email fraud attacks](https://www.proofpoint.com/us/blog/threat-protection/email-fraud-continues-rise-number-attacks-grew-36-q2).

When you typically send an email, the “from” field is automatically filled out. If my email is john\_johnson[@]gmail[.]com, and I send an email to my friend, my friend will see that the email came from my email address. However, you can also send emails with simple scripts (here are [instructions for sending an email in Python](https://realpython.com/python-send-email/)).

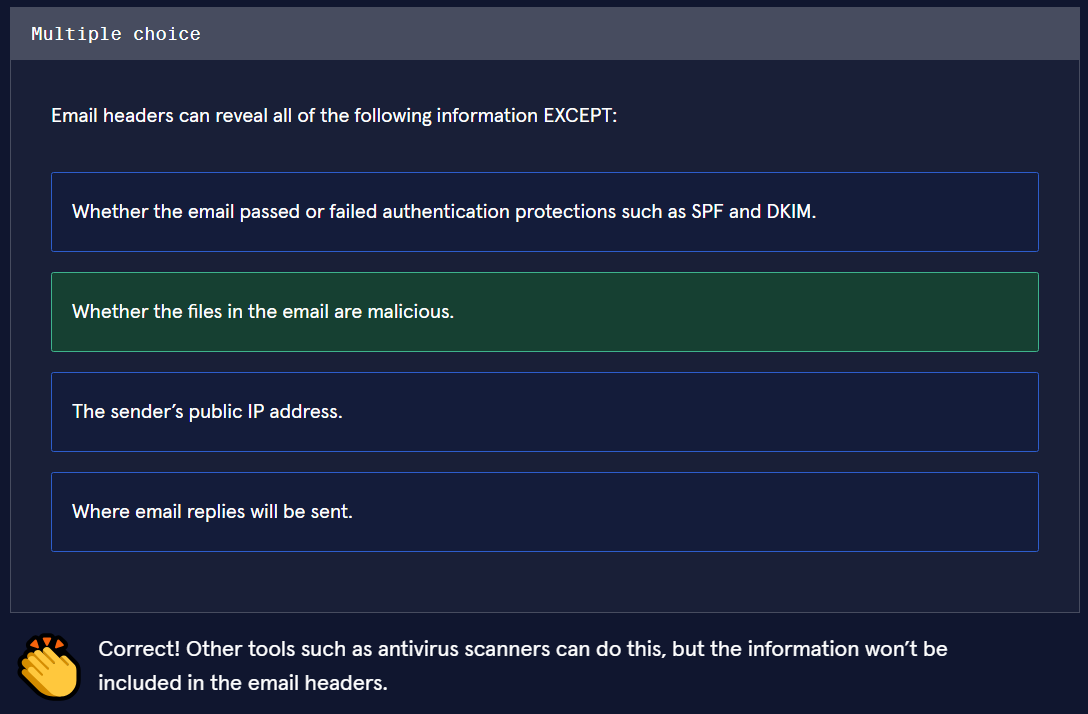
When you write and send an email using a programming script, you can configure the email headers to be whatever you want - meaning that an attacker can put any email as the “sender”, even yours. In order to really see what is going on in an email, you can download it and open it in a code editor, but most email providers allow you to see the email headers from within your email. For example, in Gmail, if you open an email of interest, click on the three vertical dots in the upper right-hand corner, and click on “Show original”, you can see the email headers.



These email headers provide valuable information that can help detect phishing, such as the “return-to” address, sender IP, and whether the email failed any protections such as [SPF and DKIM](https://www.csoonline.com/article/3254234/mastering-email-security-with-dmarc-spf-and-dkim.html), which help to fight spoofing (they are the reason emails are automatically sent to your spam folder). If you see a suspicious email, it is always wise to open the headers before responding in order to see if any protection fields “failed”, and to look at the original sender IP. You can read more about email spoofing [here](https://www.proofpoint.com/us/glossary/email-spoofing" \t "_blank).



The headers of a phishing email, showing that it failed SPF protections.

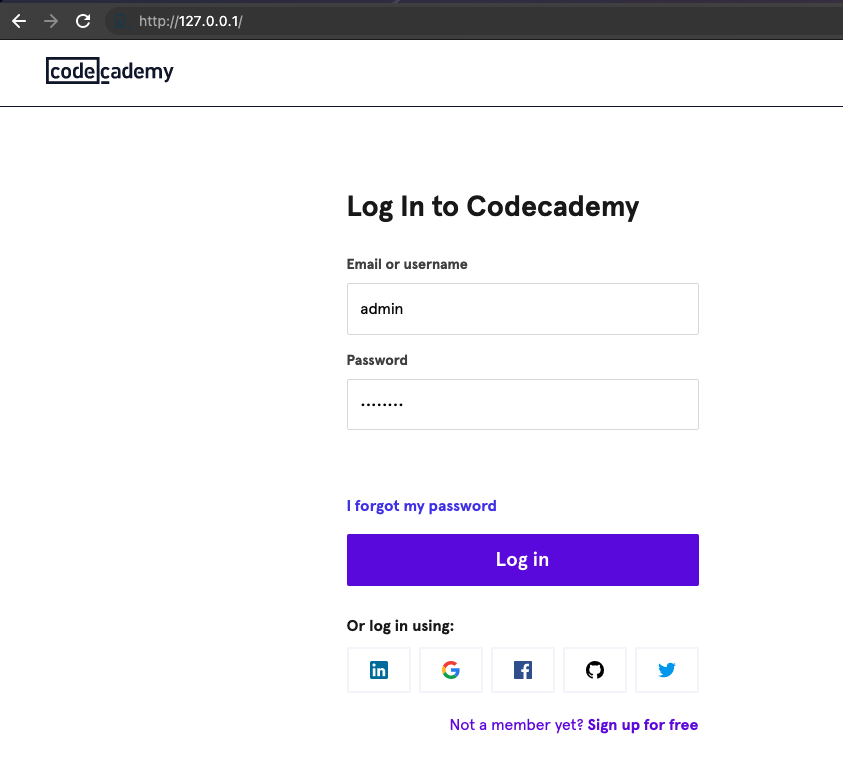


### Not Just Emails: Webpages That Steal Your Password

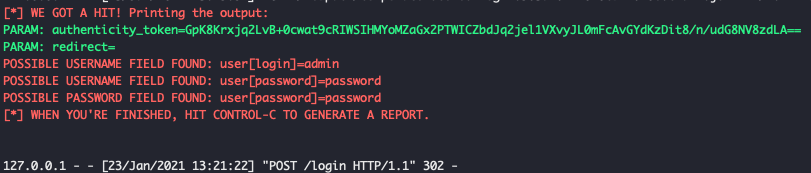
Webpages that harvest credentials are especially effective phishing tools. Because these pages often forward victims to a legitimate webpage after stealing their login information, the user never realizes they were phished. These webpages can also encourage you to download malware unknowingly.

If someone were trying to steal Codecademy logins they could occupy a [typo-squatting](https://www.upguard.com/blog/typosquatting) domain like **codecademy.cm** or **codeoademy.com** in the hopes that a user would accidentally type in the wrong domain. A malicious actor could also disguise their domain with a link shortener like [bitly](https://bitly.com/" \t "_blank) to get someone to click through to a disguised domain.

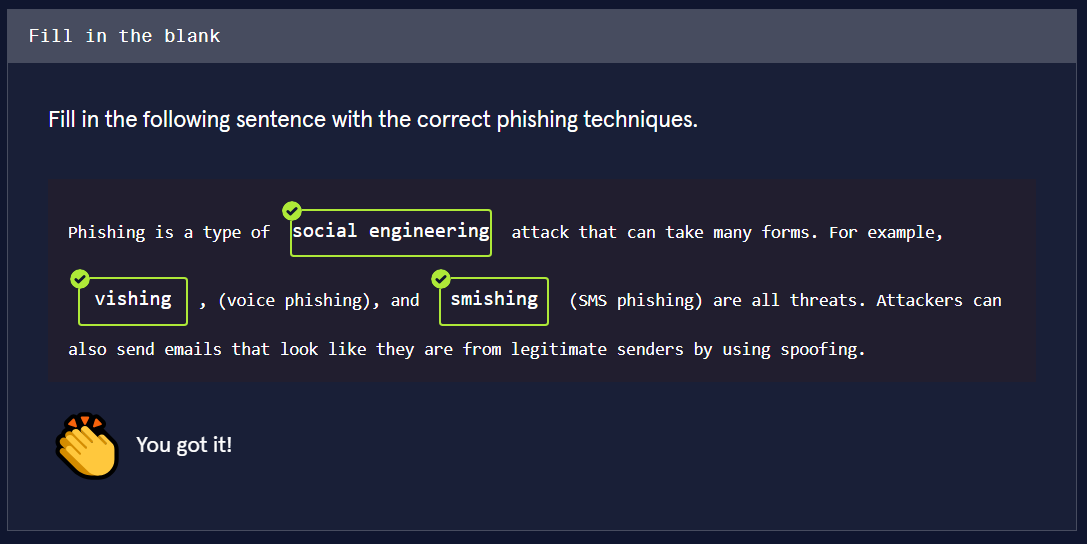
Below, we’ve set up our own credential harvesting webpage that looks identical to the Codecademy login page. We did this by downloading the HTML files for Codecademy. In the screenshot, the page is on a local server we can monitor, but we could choose to host it on any domain we owned.



When someone lands on this page, they think it’s the real **codecademy.com**! When they enter their username “admin” and password “password” and log in, that login information gets sent to our backend.



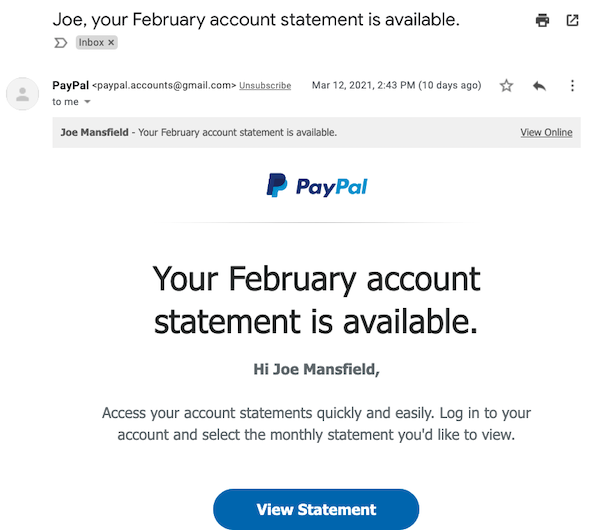
Because we can program the “Log in” button to redirect to the real Codecademy page, unless a potential victim had looked at the domain and noticed that something was off, they would have had no indication that the page just sent their information to us. This is one potential way that an attacker can use a website to trick someone into handing over their credentials. It seems like there are a million ways we can be expertly deceived on the web. Let’s talk about how to detect these!



## Detection Techniques

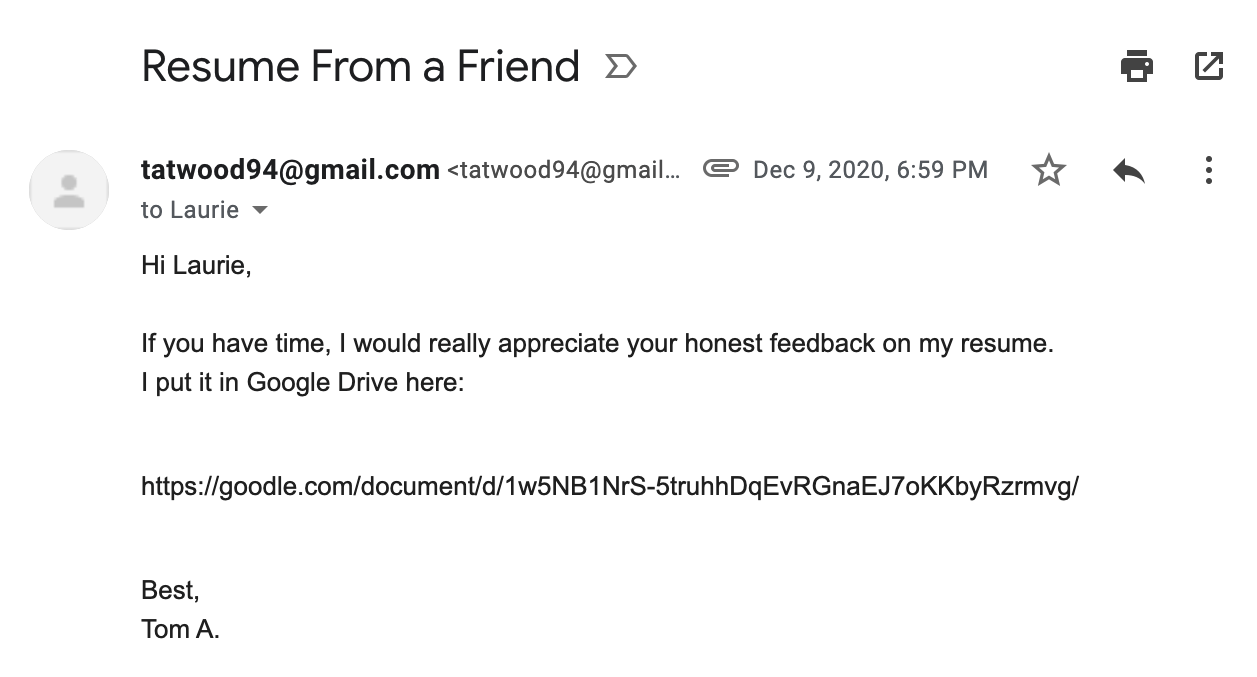
Fortunately, there are ways that we can train both ourselves and our organizations not to fall for phishing! Although many phishing websites are near copies of the originals, phishing emails can be easier to spot. Below are three examples of phishing, two emails and one webpage. Can you spot the indications on each that it isn’t legitimate?

### Example One:



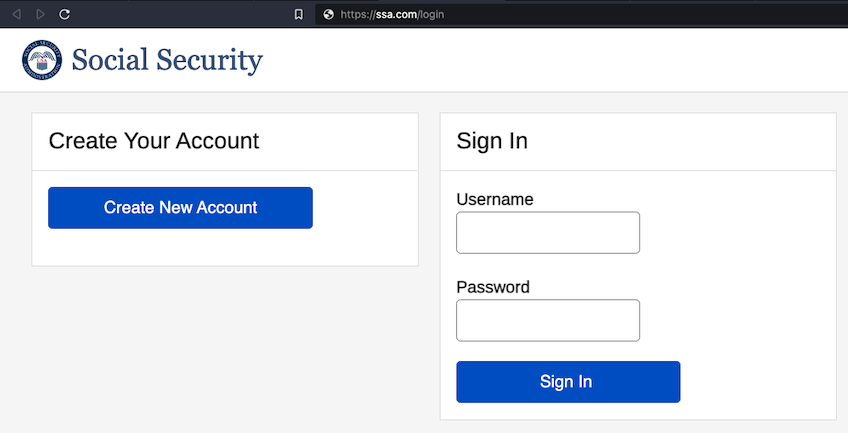
This one is pretty convincing. Did you spot the giveaway? The sender is paypal[.]accounts@gmail[.]com. Remember, anybody can register a @gmail.com address. The real PayPal will always use a business domain: @paypal.com. Another method? You can open [developer tools](https://www.codecademy.com/articles/use-devtools) on any buttons in an email to see where they are taking you. Developer tools is a cybersecurity expert’s best friend. It can reveal many secrets that attackers don’t want you to see.

### Example Two:



This is also a pretty convincing email, especially if Tom Atwood is in your contacts. In fact, once an attacker compromises an email address, they can use it to distribute more phishing emails to the people in the victim’s contacts list, utilizing **email spoofing** to make the emails appear to come from known contacts. The fact that the attacker addresses the victim by name would also make this an example of spear phishing. What’s the giveaway here? Take a closer look at that URL - the second “g” in “google” is really a “d”. This means that the link is probably taking you to a malicious fake website which will ask you to log in to Google Drive and steal your credentials.

### Example Three:



This webpage is very similar to the real Social Security webpage, visible [here](https://secure.ssa.gov/RIL/SiView.action). However, two things are a bit off. Firstly, all official U.S. government websites should have a **.gov** domain, not a **.com**, and secondly, have you ever seen a username and password field without an option for “forgot password?” Looking at the domain will probably provide the best information, but paying attention to small details such as missing or malfunctioning buttons, and grammar or punctuation mistakes, are key in identifying phishing pages.

