**Phishing**

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

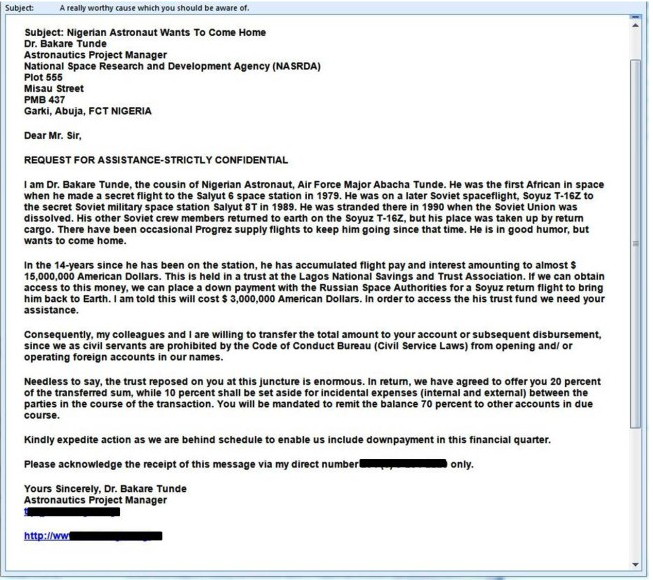
*Note: Attempting to phish the credentials of someone without their express consent is illegal. The information presented in this course in no way encourages or condones phishing, and should not be used to attempt a phishing attack.*

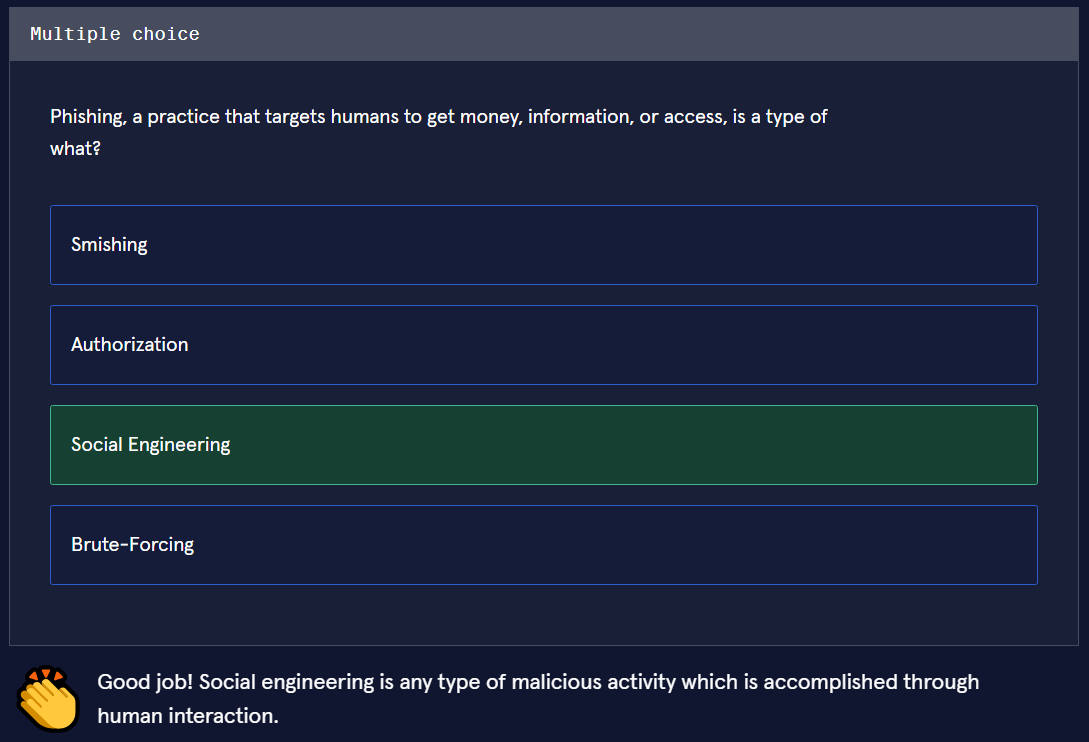
Phishing is one of the most well-known types of cyber attacks. The average internet user has never heard of Kali Linux or written Python scripts to guess passwords, but everyone knows not to respond to an email from a down on their luck Nigerian Prince (well, [almost everyone](https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollar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

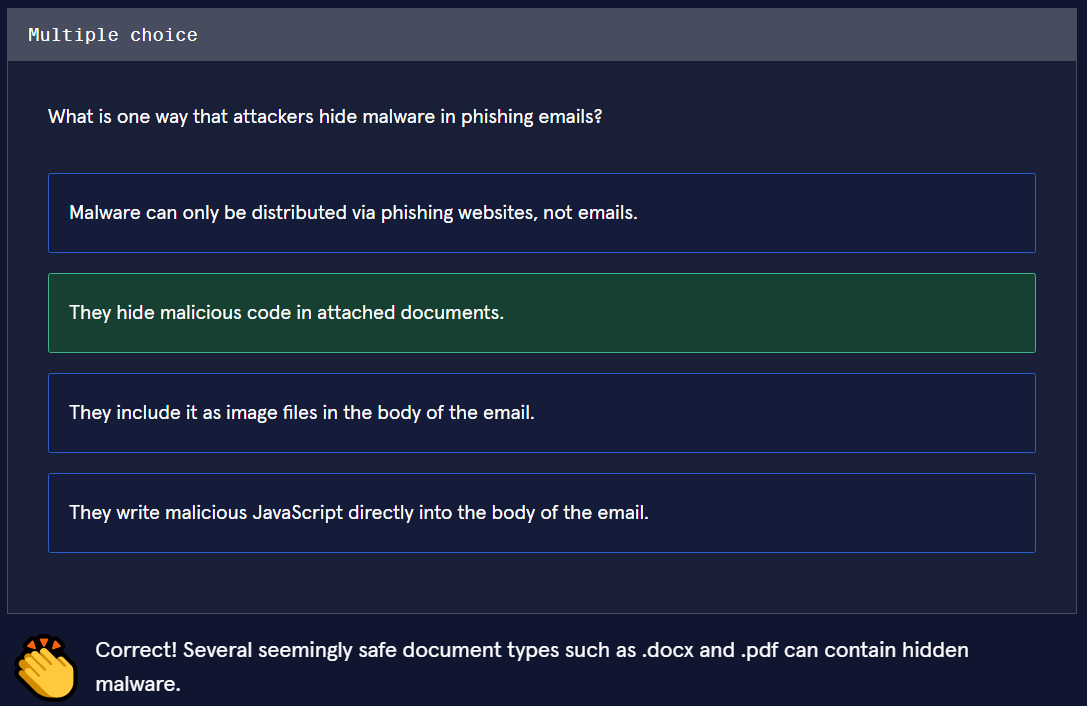


## How Does Phishing Work?

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.

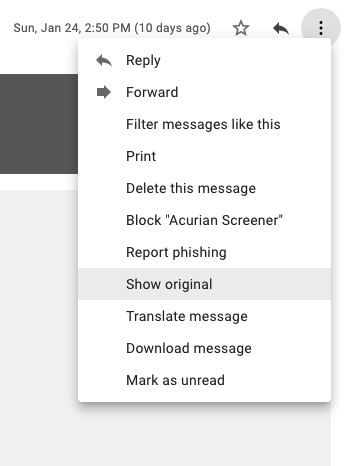


### Email Spoofing

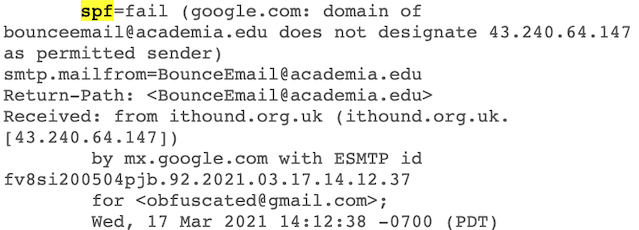
Email spoofing refers to when an attacker falsifies their email headers to make it appear as though the email is coming from someone else. Spoofing is a common component in phishing emails, used in as many as [90% of email fraud attacks](https://www.proofpoint.com/us/blog/threat-protection/email-fraud-continues-rise-number-attacks-grew-36-q2).

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.

