

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](#)).

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](#).

Sometimes phishing attacks can seem comically implausible, such as this [phishing email from an unfortunate astronaut lost in space](#) below. However, with phishing attacks becoming both more common and more sophisticated, it's vital to be able to identify and stop phishing attacks.

Subject: A really worthy cause which you should be aware of.

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [REDACTED] only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager

[REDACTED]

[http://www.\[REDACTED\]](http://www.[REDACTED])

Multiple choice

Phishing, a practice that targets humans to get money, information, or access, is a type of what?

Smishing

Authorization

Social Engineering

Brute-Forcing



Good job! Social engineering is any type of malicious activity which is accomplished through human interaction.

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](#) (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](#) (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](#). If the target is extremely sought after, like the CEO of a company, it is known as [whaling](#).

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.

Multiple choice

Which of the following is NOT a type of phishing?

Smishing

Vishing

Sealing

Whaling



Correct! All of the other terms here are a type of phishing.

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.

Multiple choice

What is one way that attackers hide malware in phishing emails?

Malware can only be distributed via phishing websites, not emails.

They hide malicious code in attached documents.

They include it as image files in the body of the email.

They write malicious JavaScript directly into the body of the email.



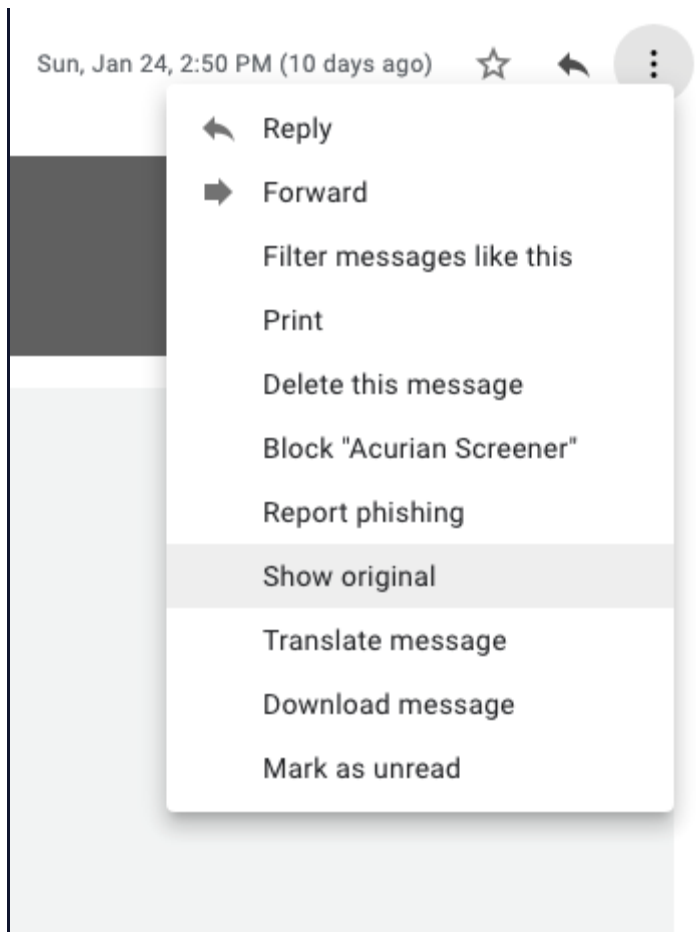
Correct! Several seemingly safe document types such as .docx and .pdf can contain hidden malware.

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](#).

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](#)).

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](#), 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](#).

```
spf=fail (google.com: domain of
bounceemail@academia.edu does not designate 43.240.64.147
as permitted sender)
smtp.mailfrom=BounceEmail@academia.edu
Return-Path: <BounceEmail@academia.edu>
Received: from ithound.org.uk (ithound.org.uk.
[43.240.64.147])
    by mx.google.com with ESMTP id
fv8si200504pjb.92.2021.03.17.14.12.37
    for <obfuscated@gmail.com>;
    Wed, 17 Mar 2021 14:12:38 -0700 (PDT)
```

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

Multiple choice

Email headers can reveal all of the following information EXCEPT:

Whether the email passed or failed authentication protections such as SPF and DKIM.

Whether the files in the email are malicious.

The sender's public IP address.

Where email replies will be sent.



Correct! Other tools such as antivirus scanners can do this, but the information won't be included in the email headers.

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](#) 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](#) 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.

← → ↻ http://127.0.0.1/

codecademy

Log In to Codecademy






Email or username

Password

[I forgot my password](#)

Log in

Or log in using:



[Not a member yet? Sign up for free](#)

When someone lands on this page, they think it's the real [codecademy.com](https://www.codecademy.com)! When they enter their username "admin" and password "password" and log in, that login information gets sent to our backend.

```
[*] WE GOT A HIT! Printing the output:  
PARAM: authenticity_token=GpK8Krxjq2LvB+0cwat9cRIWSIHMYoMzaGx2PTWICZbdJq2jel1VXvyJL0mFcAvGYdKzDit8/n/udG8NV8zdLA=  
PARAM: redirect=  
POSSIBLE USERNAME FIELD FOUND: user[login]=admin  
POSSIBLE USERNAME FIELD FOUND: user[password]=password  
POSSIBLE PASSWORD FIELD FOUND: user[password]=password  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

```
127.0.0.1 - - [23/Jan/2021 13:21:22] "POST /login HTTP/1.1" 302 -
```

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!

Fill in the blank

Fill in the following sentence with the correct phishing techniques.

Phishing is a type of ☒ **social engineering** attack that can take many forms. For example, ☒ **vishing**, (voice phishing), and ☒ **smishing** (SMS phishing) are all threats. Attackers can also send emails that look like they are from legitimate senders by using spoofing.

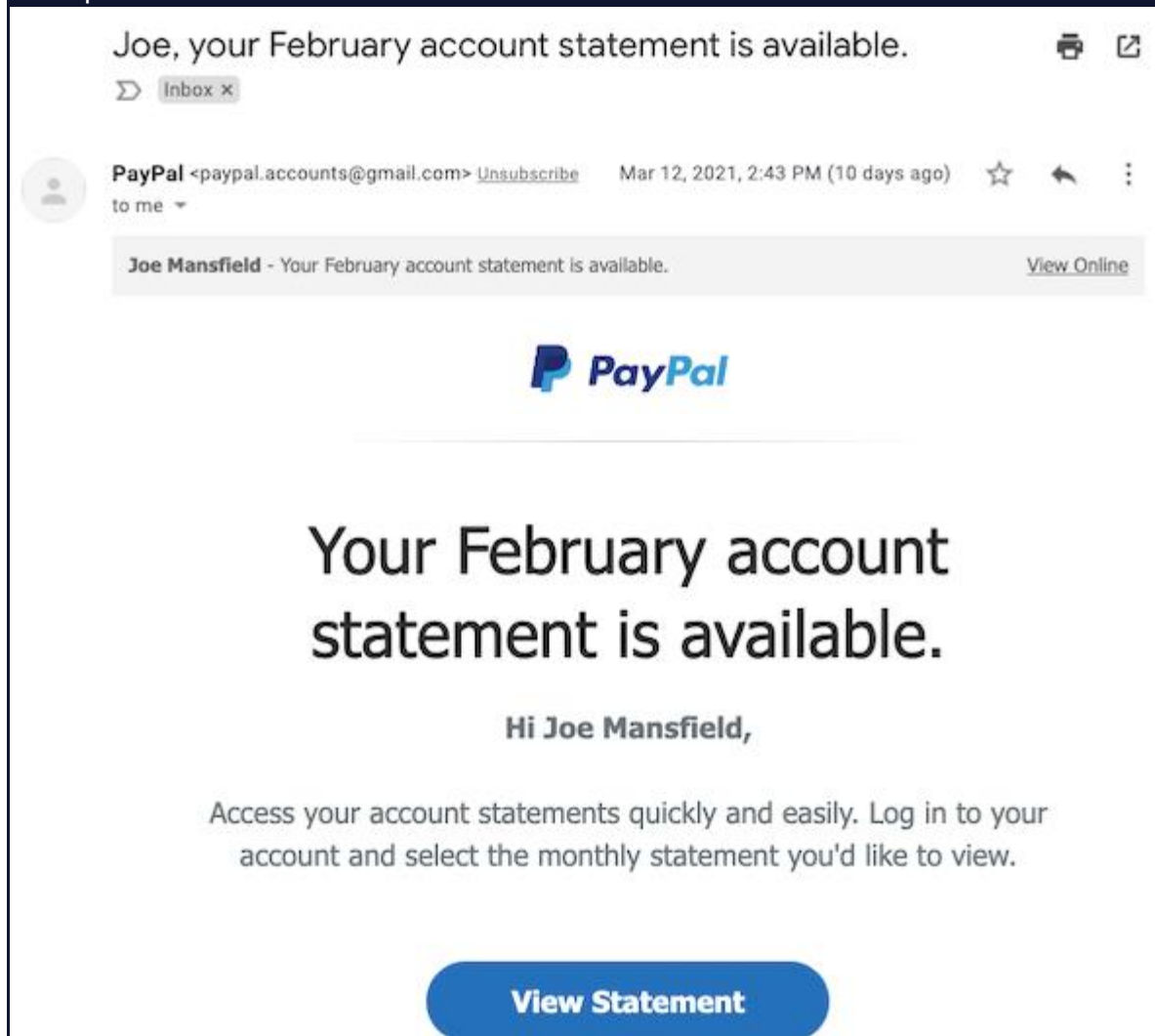


You got it!

Detection Techniques

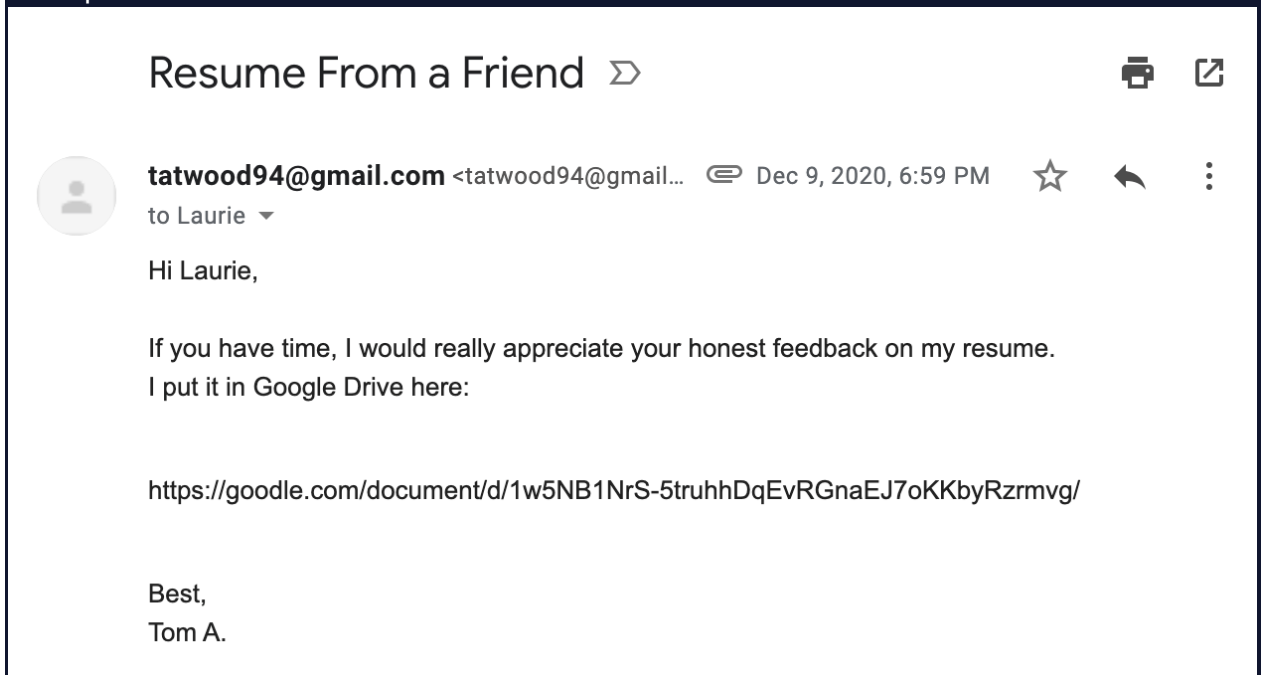
Fortunately, there are ways that we can train both ourselves and our organizations not to fall for phishing! Although many phishing websites are near copies of the originals, phishing emails can be easier to spot. Below are three examples of phishing, two emails and one webpage. Can you spot the indications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

Example One:



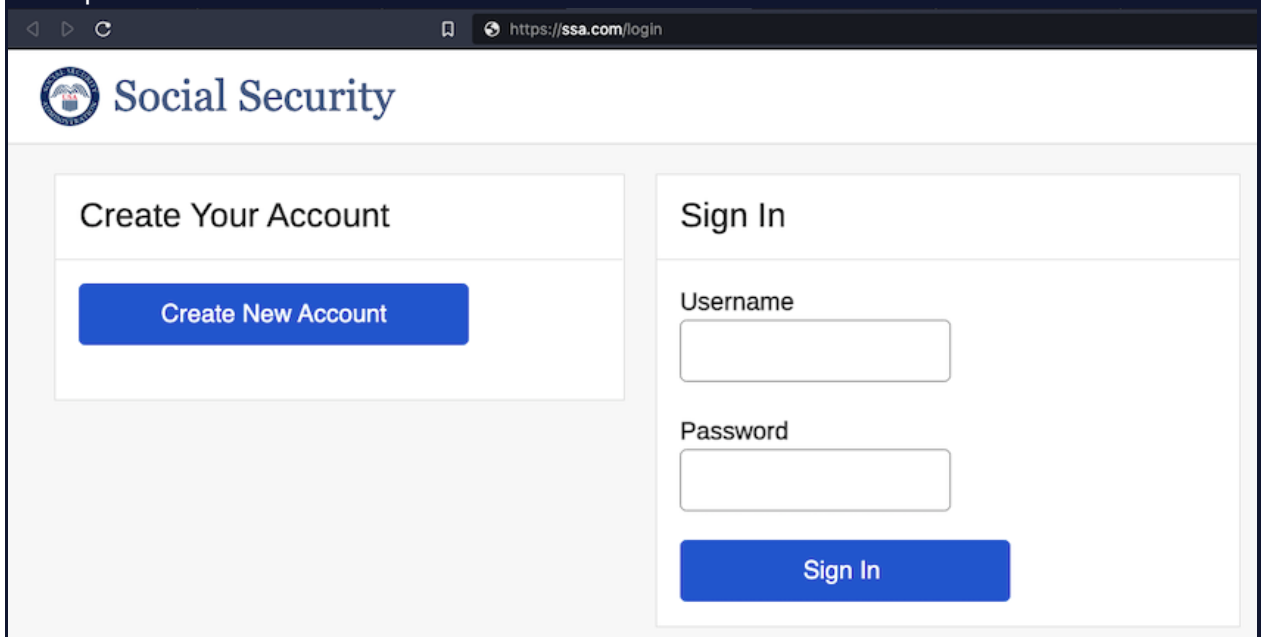
This one is pretty convincing. Did you spot the giveaway? The sender is paypal[.]accounts@gmail[.]com. Remember, anybody can register a @gmail.com address. The real PayPal will always use a business domain: @paypal.com. Another method? You can open [developer tools](#) on any buttons in an email to see 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](#). 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.

Multiple choice

What are some ways to spot phishing webpages?

Look for punctuation errors and suspicious URLs.

Check to see if the site or email is from a domain that doesn't end in [.com](#).

Look for a copyright symbol to indicate the page is legitimate.

Look for embedded content such as a map or a video.



Correct! Punctuation errors are more common than spelling errors since they won't usually be caught by spell check.

Conclusion and Further Reading

The variety of phishing types, the low cost to create phishing pages, and the ease with which someone can create one, all make phishing a difficult threat to counter. Additionally, regardless of how complex a system is, no system in the world can guarantee against a human employee clicking on a malicious link. This is why it is important to always report suspicious emails or links at work to the appropriate department so that they can block suspicious senders and domains. If you are paying attention to small details and reporting suspicious content, one person can do much to protect an organization and themselves against phishing attacks.

While we've talked about some strategies for phishing, you should never use them to harm others. If you're on the security team at your work, you could run a phishing campaign to see if employees know what types of content to avoid.

Want to Learn More?

You can use certain tools like [Passive DNS](#) to find real live phishing pages online, or check out [some real examples of phishing campaigns](#). You can also see them in your email's spam folder, and even examine the email headers to see where the mail is coming from, but be careful not to click on anything! Finally, you can check out [some](#)

[famous phishing attacks](#). Phishing is everywhere - but if you equip yourself and equip others, you should be safe!