**Intro to Cybersecurity**

* Social Engineering is any type of malicious activity whic is accomplished through human interaction.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Different Types of Phishing**

* *Vishing:* from voise phising, 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.

Phishing is also categorized by who it targets. **Spear phishing:** when an attacker has a specific target in mind and sends the target a dedicated, personalized email. If the target is extremely sought after, like the CEO of a company, it is known as **whaling.**

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

**How Does Phishing Work?**

Phishing attacks can be emails or phone calls that attempt to get a victim to send an attacker money or payment information. Phishing also can be related to when attackers get people to click on links that download malware onto their systems. 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.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**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.

When you typically send an email, the “from” field is automatically filled out. However, you can also send emails with simple scripts.

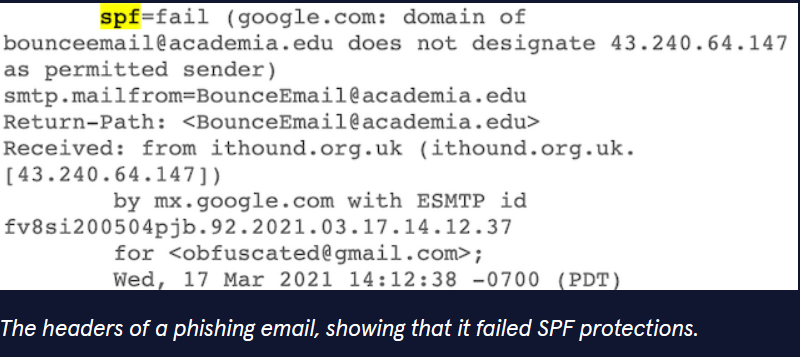
When you write and send an email using a programming script, you can configure the email headers to be whatever you want – meaning that an attacker can pu any email as the “sender”, even yours. To really see what is going on in an email, you can download it and open it in a code editor, but most email providers allow you to see the email headers form within your email. 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.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

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 reasons emails are automatically ent to your spam folder).

More on email spoofing - > <https://www.proofpoint.com/us/threat-reference/email-spoofing>



**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 a disguised domain.

When someone lands on a fake page, they think it’s the real webpage. When they enter their username “admin” and password “password” and log in, that logint information gets sent to our backend (they are giving a fake webpage of the original codecademy webpage as an example).

Texto

Descripción generada automáticamente

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 notices that something was oof, 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.

Captura de pantalla de un celular

Descripción generada automáticamente

**DETECTION TECHNIQUES**

Below are three examples of phishing. Can you spot the indications on each that it isn´t legitimate?

**Example one**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Giveaway: the sender is [paypal.accounts@gmail.com](mailto:paypal.accounts@gmail.com). Remember, **anybody can register a @gmail.com address.** The real PayPal will always use a business domain: @paypal.com.

**Example Two**

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

This is also a 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 (hackers focused on an specific individual). **The giveaway: 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**

**Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente**

**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 a 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.

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente