# Phishing: No License Required

In the world of cyber crime, phishing remains one of the most consistent and successful tools for gaining access to a computer or network. Its range of use is vast. It’s employed by the most sophisticated and organized of cyber crime groups — including state-sponsored cyber crime groups — right down to the most unsophisticated and disconnected of hackers, the loners living in their parent's basements. Phishing has been a key step in some of the biggest heists in cyber crime history, most notably the theft of $81 million US dollars from the Central Bank of Bangladesh. It's a standard tool for gaining access to credit and debit card information as well as a plethora of personal information that can easily be sold in the black markets on the dark web.

## What is Phishing

Phishing, in its simplest definition, is the use of an email to entice or convince the recipient to click on an attachment or follow a set of instructions on a web page accessed through a click-through URL. In either case, the attachment or the web page, the recipient is susceptible to intrusion into their computer or network system, whether that system is your home computer, which might contain more passwords and more access for the hackers, or your work network, which opens your professional network to the hackers. Phishing is one of the oldest and most consistently successful tools used by hackers.

A basic and common example of phishing is the phony email from PayPal™. Your payment information is not up to date. Would you *please* go to the following URL and update your payment information to continue using PayPal, or it could be a threat alert. Your PayPal account might be compromised. There was a suspicious login from Indonesia. Was this you? This emotional imperative is used often. They want to scare you into thinking you have already been hacked, and you could lose money. Of course, the website you are directed to is not the official PayPal website, and you were duped into giving the information to log onto your PayPal account to the fraudsters. It can happen fast — boom, boom, boom — like firecrackers going off. How hard would it have been to thwart? Contact PayPal, or go to their real website and log in to verify that your payment details are incorrect. In fairness to the victims, the emails can be quite official looking — correct logo, correct personal information for you, and other indicators that you can trust the message and, therefore, the attachment or URL.

## The Variety of Phishing

There are phishing scams for all kinds of different demographics, the old, the Young, pensioners, and successful businesses. Data aggregated year in and year out suggests that nobody is immune and phishing scams are growing every year. Cybercrime is so widespread that even the Department of Homeland Security is involved in the United States. It’s not the same old stunt over and over again. Phishing is in a constant state of evolution, adaptation, and growth in sophistry. The more diligent practitioners of phishing take their time to case a subject whom they want to target. This could include numerous hours of monitoring and surveilling their social media platforms for deeper insight into the target. This insight can then be used to *personalize* the email in some way, to intimate familiarity, which takes down the defenses of the target and makes them feel secure in clicking on the link or attachment. They are criminals, but they do due diligence.

Cyber security experts now train and advise people on what they post on social media. The use of social media was an integral part of the attack on the Central Bank of Bangladesh. Your social media profiles — Facebook, LinkedIn, Twitter (X), and Instagram — allow cyber criminals to understand you and present themselves as familiars. The number one rule: do not post any work-related data on your social media platforms.

## Criminal Evolution

As technology evolves, so does cyber crime. The advertising industry is beginning to significantly define time and geography-delimited digital advertising on mobile devices. This is done through collecting device IDs and the geographic location of the user, all of which are commercial data products collected and sold now in the legitimate business world. For example, you’re walking towards a subway platform after work.

It’s a late Wednesday afternoon, maybe 5:15 PM, and you get an advertisement on your phone for a coffee from your favorite coffee shop, which, non-coincidentally, you just happen to be walking past on your way to the subway stop, and the advertisement is for a coffee you love, which they know because you’ve bought it numerous times in the past using your — *yeh, you got it* — your telephone as the electronic payment instrument, and all this manufactured synergy was gathered and strategically deployed to produce an effective advertisement on your phone, effective because you bought the coffee. Now, imagine this same cutting-edge advertising technique employed in phishing. Do you see where this is going?

## Commercial Phishing

If the lone operator in his mom’s basement, or the small groups of competent cyber criminals were not enough, we now have the age of commercial phishing, an almost one-to-one match for the actual trade of ocean fishing. The loan operator would be like the old Cuban man in Ernest Hemingway’s *Old Man and the Sea*, and the commercial phishing operations are like Chinese or Portuguese deep-sea fishing boats with huge nets. There are vendors now selling services for Phishing as a Service (PaaS).

In the second quarter of 2023, cyber security experts became aware of a product called *Greatness*. Cisco™ reported the following in a security blog it posted on May 10, 2023.

“A previously unreported phishing-as-a-service (PaaS) offering named *Greatness* has been used in several phishing campaigns since at least mid-2022. Greatness incorporates features seen in some of the most advanced PaaS offerings, such as multi-factor authentication (MFA) bypass, IP filtering, and integration with Telegram bots. Greatness, for now, is only focused on Microsoft 365 phishing pages, providing its affiliates with an attachment and link builder that creates highly convincing decoy and login pages. It contains features such as having the victim’s email address pre-filled and displaying their appropriate company logo and background image, extracted from the target organization’s real Microsoft 365 login page. This makes Greatness particularly well-suited for phishing business users.”

This, to be sure, is the first of many offerings to be made in the area of commercial fishing.

It will be nearly impossible to stop the sale of this type of software on the dark web. It’s been nearly impossible to stop the sale of almost everything else on the dark web.

## Proceed with Caution

Your defense is your responsibility, whether you are an individual computer user or an employee at a larger corporate entity. The main defense is training. Most organizations now will have a security department that regularly monitors and stays abreast of what the latest online scams are, and, as part of their function within the larger organization, they train the rest of the employees. This training should be current and up to date. New phishing attack methods are being developed all the time. Make sure that all of your employees understand the basics of the World Wide Web. Train them to never give their information to an unsecured site. The URL must begin with https, and you should be able to see a closed padlock icon next to the URL. This may seem a bit excessive because not every site without a security certificate is a scam, but better safe than sorry, especially when you’re operating from a work computer and allowing risk to the entire network. It's very important that your organization set up a password rotation schedule and remind employees of emails. Regular online training courses should be taken by employees, and either developed in-house by the documentation and training team or outsourced to reputable vendors with a solid track record. Nothing is going to secure your network better than a trained and educated workforce. This has been standard practice in the financial sector for well over two decades, but it needs to be adopted in all industries.

The other thing you can do to protect yourself is to invest in technology and tools, especially if you interact with the public online, and this could be as innocuous as taking in information. Always make sure they’re human. Bot access to your system is another type of phishing but backward. Rather than you going to the scam through an attachment or a URL, the scam comes to you in the form of a bot, but once that bot gains access to your system it can do the same damage as the phish. It's a known fact in the cyber security world that multi-factor authentication (MFA) is a critical component in hindering phishing and other types of online crime, but not all MFA products are equal. Just as you now know platforms like Greatness can bypass weak MFA tools, you should also know that not all MFA tools are the same. Some are hollow and one-dimensional. Others, like hCaptcha™, are cutting-edge in the use of machine learning (ML) and artificial intelligence (AI). You have to protect yourself intelligently, and what better way than AI and ML?