Phishing is a type of security threat where a threat actor will send counterfeit emails (that look real), to lure victims into giving their username, passwords and other sensitive information to the threat actor. One place where this occurs commonly is in the work place or school organizations. Emails are sent that seem like it could be from a fellow business partner, student or organization. I have not received any suspicious emails for work, mainly because I work in a restaurant and there is little to no need to use a work email. However, since I’ve started college, I have received many emails, almost seems like once a week, there is a new phishing email that gets sent to my school email account. This not only has happened here at West Chester, but also at the community college I transferred from.

Most of these phishing emails I received were, almost everytime, something to do with either a part time student job paying a generous amount of money per week, or regarding an internship opportunity. The phishing emails I’ve received on my school email account are pretty dangerous. Not because of what the hacker is going to do with the information, but these emails look nearly legitimate. My personal email account gets so many fake and phishing emails, and they all just end up in my junk mailbox, so I hardly ever see them. With the ones I’ve seen recently here at West Chester, they are revied in the main inbox, so the spam filter doesn’t recognize this email. Most times, if something comes into my main inbox, I usually believe its real.

The emails that have been sent by hacker’s have nearly fooled me. I have almost clicked on some of them this semester. These emails are so dangerous because I am someone who has been studying cybersecurity for two semesters now, and it’s almost got me. Another issue is that by the time IT picks up on it, the email has been out for a few days. It is possible to accidentally click the email, and if the hacker is looking to get something related to your IP address, they definitely can.

Back to the article, there are many different things the hacker can do once they obtain a victims information. Organized crime plays a large part in cyber crimes, and the black market is their marketplace to sell. Good news is that there are antivirus that check the Dark Web to see if your social security number has been exposed, and removes it. One analyst, Avivah Litan with Gartner Inc, a research firm, arrived at the conclusion that in 2004 that “there were 1.8 million phishing attack victims, and the fraud incurred by phishing victims totaled $1.2 billion.” (David Geer). Another firm, Delivery Channels Research Service with senior analyst George Tubin, estimated the total cost of preventing cyber-attacks, such as using antivirus and antiphishing technology, and educating users came up to a total of $100 million dollars.

This article is almost 17 years old, however, most of the concepts still apply to today’s cybersecurity practices. Many anti phishing and tactics to fight phishing attacks started around this time. There’s a few older practices that I never realized could have such an impact, and nowadays, are probably automated tasks. For example, one way to avoid phishing attacks is for the ISP to shut down the site. If a victim accidentally clicks the link and is redirected to the website, nothing will happen because the website won’t exist anymore. I don’t have any facts to support this, but I believe that ISPs use some type of automation to compare real sites to phishing sites. The team of analysts will then review the fake sites, and disable them if they find a violation.

Another way that several anti phishing companies will combat hackers is by using retaliatory services, or basically fighting fire with fire. I’ve seen this done on YouTube or Discord where someone will try to scam or phish a well-experienced cybersecurity professional. The cybersecurity professional ends up doing a retaliation towards the hackers. In the article, the anti phishing companies will flood the phishing websites with fake credit card numbers and fake credentials that can’t be used. The one tactic I saw online was from a fake marketplace website, similar to something like Amazon, that used a real credit card authentication service. The cybersecurity professional wrote a program out in Python, and flooded the website with fake credit card numbers and information. The way this affected the hacker was that every time the credit card authenticator was used, the host of the website (the hacker) was charged a fee. So basically, the cybersecurity professional made the hacker pay out a lot of money in these fees. The hacker couldn’t do anything about it because his business was illegitimate.