Francisco Cilia, Jan Bermudez, José Renteria

The problem that we want to focus on this term is Phishing. Known as the most common form of cyber crime, with an estimated 3.4 billion emails a day sent by cyber criminals (Smith). This is one of the most prevalent threats that individuals and organizations alike face. Attacks usually involve deceptive tactics from malicious actors that aim to trick users into giving up sensitive information (i.e. usernames, passwords, banking information). Over the last few years we have seen sophisticated attacks increasing at an alarming rate, and as the frequency continues to go up there is an urgent need to address this pressing issue. Our team aims to dig into the intricacies of phishing attacks, understand the latest trends, and propose a strategy to improve awareness and prepare defenses against this growing cyber threat.

Currently, organizations use a combination of email filtering, security awareness training, and multifactor authentication as defenses against phishing attacks. Although these measures offer some protection within work environments, there's still a critical gap that exists outside of the professional realm. People are usually well prepared to identify these cyber attacks in work-related communications; however, the same level of awareness is simply not the same in personal and non-professional contexts. This poses a significant vulnerability that bad actors exploit. Hence, there is an essential need to bridge this awareness gap and extend protective practices to all facets of user's digital lives.

Some current prevention techniques involve installing security software that can filter emails and other potential scams. While this will almost certainly catch low hanging fruit, it struggles with complexly crafted attacks that require user input. It is a good idea though, to keep your auto-updates on so that it can keep up with ever-evolving threats. Turning on auto-updates for your mobile OS is also a good idea for the same reason. Most business applications and anything that holds sensitive information will usually offer a form of multi-factor authentication. Backing up your data, whether locally on a hard drive or to the cloud is also a good prevention technique, should your data be breached or lost.

The main problem that makes phishing so prevalent is the fact that there are no laws denoting it as a crime, and thus no punishment for anyone doing it, unless it falls under the category of wire fraud or another legally punishable offense. There is not much awareness regarding phishing even in recent years, and most people working in businesses are too trusting and do not believe it could happen to them so easily. Humans are good at being tricked, as we believe what our eyes tell us, and phishers have learned to exploit this in order to get people to act against their own interests.

Our current action plan begins with the first week conducting a literature review on current prevention methods and their effectiveness. This can be followed up with a survey asking peers if they've ever been victim to a phishing attack and what they think made the attack successful. The second week would consist of methodology and algorithm design to defend against the method of attack. This could come in many forms including a browser extension, a website providing user awareness, or a URL scanner. The following next two weeks until the midterm report will be dedicated to implementing the selected solution. Roles are subject to change but begin with all members conducting literature review and a peer survey to gather data. Then depending on the selected solution we can have roles for the front-end, backend, database management, UI design, ML and project manager to ensure milestones are met. Deliverables include a complete project report, a final version of the project presentation, and code with associated documentation.

Works Cited

Gary Smith, et al. “Top Phishing Statistics for 2024: Latest Figures and Trends.” StationX, 12 Dec. 2023, www.stationx.net/phishing-statistics/

https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams