Protect Yourself Online Memo

To: Dr. Lane

From: Matt Childrey

In 2019, it isn't just about using padlocks and deadbolts to protect yourself and your personal belongings. As Memphis grows into a connected and innovative city, it is also important that it ensures its citizens can grow safely with it in the online world. A great way to do this would be by running an online social awareness campaign that targets threats, such as Phishing and Robocalls, and also informs Memphians of ways to defend against them, like Two-factor Authentication and Technological literacy advocacy.

In June of 2018, the U.S District Court for the Western District of Tennessee filed cybercrime charges against several international individuals in coordination with other federal agencies, all as a part of a coordinated effort titled *Operation Keyboard Warrior*. The reason this was occurring here in Memphis is because one of the victims, named as *Company A* in the indictment, was a real-estate company from our city. The defendants committed "a series of intrusions into the servers and email systems,"[1] which included tasks as simple as using a "spoofed email," yet they stole at least six figures from the Memphis economy.

---

[1] US Attorney's Office Western District of Tennessee. *Eight Arrested in Africa-Based Cybercrime and Business Email Compromise Conspiracy.* June 25, 2018. https://www.justice.gov/usao-wdtn/pr/eight-arrested-africa-based-cybercrime-and-business-email-compromise-conspiracy

And while there is now a history of large incidents of cyber fraud in the Memphis area, there is also evidence of it affecting citizens in more normal circumstances. In just May of this year, the Federal Communications Commission had to warn Americans after it noticed it an uptick in robocalls with a distinct West African area code and scam technique. In that warning, Memphis and it's 901 cellular telephone code was ranked as the 5th most targeted area for the scammers.[2]

As a doctrine, Social Design wants designers to actively try to "effect tangible change to make life better for others," and in this situation, we feel it is important to use design as a precautionary and informative warning against cybercrime for those that live in the Memphis area. While the issue at hand may not be a necessarily local one, it is still important to focus on the specific community at hand here. For one, it is the community we grew up and currently live in, which adds an extra level of responsibility, at least when compared to the entirety of the online ecosystem. Yet, secondly, it is critical to understand that the progressive nature of technological literacy lies hand in hand with the ability to subvert these crimes. And that's an aspect of Memphis's education system and economy that is currently lacking. Lastly, this is still a relatively new problem for people to recognize, and there hasn't been a campaign of this kind in the local area yet. An initial step forwards for awareness could do wonders for the citizens.

As mentioned in the introduction, we've already targeted specific ways that the most usual of citizens, or the every-day person, would be targeted. Phishing attacks, whether it be through email, or the now popular route of text messages. As well as Robocalls, which despite the textualization of internet communication, has actually risen in popularity over the past few years nationwide. While it is difficult to target the exact audience Phishing affects, since the range is honestly fairly large, Robocalls are statistically what the elderly population is most vulnerable to (they're about five times more likely to be targeted[3]). Advocating for an at least 10-digit with special characters alphanumeric passwords, two-factor authentication, tech literacy and precaution can help protect our community.

---

[2] Tribune Media Wires. *Report says Memphis a hotspot for 'one ring' scam robocalls*. https://wreg.com/2019/05/04/flood-of-one-ring-scam-robocalls-prompts-fcc-warning/

[3] Michelle Singletary. *Robocalls have these retirees afraid to answer their phones*. https://www.washingtonpost.com/business/2019/03/08/tech-support-scams-other-schemes-are-hitting-seniors-hard-costing-millions/