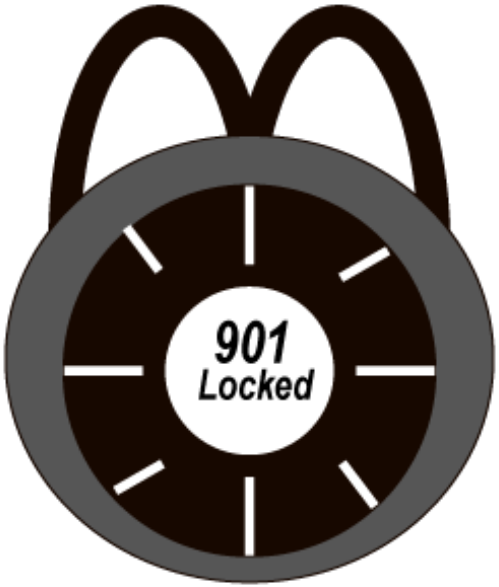
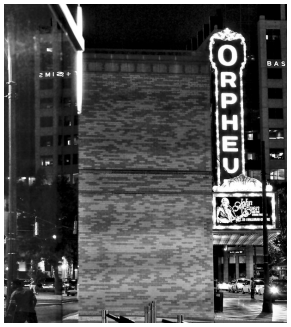
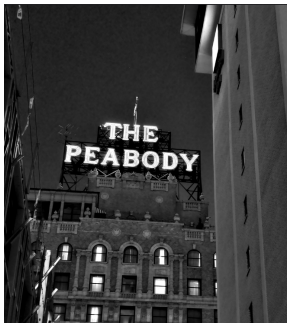
Protect Yourself Online

Campaign Guide by Matt Childrey

November 17, 2019







What's the Issue?

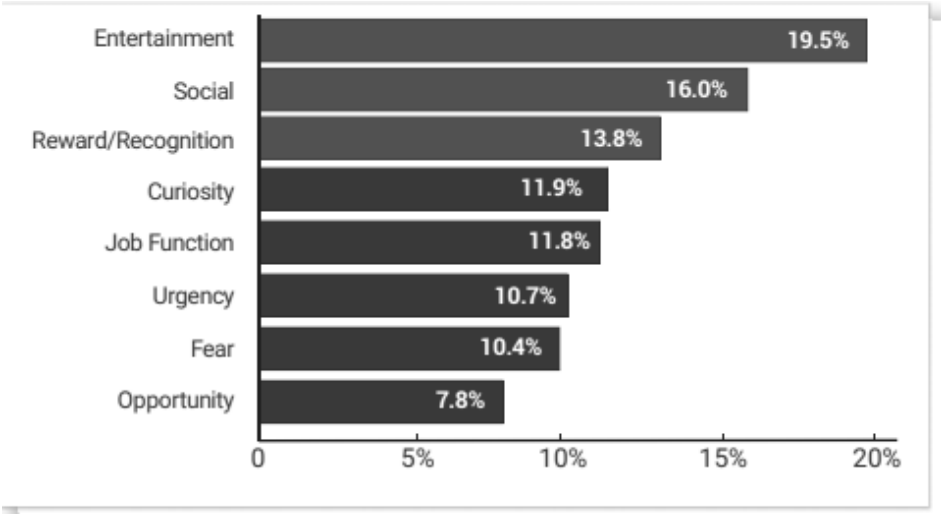
In an increasingly digital world, citizens have to practice safety just like they do everyday in real life. From the deadbolts they lock on the front door of their porch, to the passcodes they set for their iron safes, people have been exercising caution against unwanted attacks and intrusions for decades now. Yet, while these steps are still important in some ways, in many they are not. The average person's belongings are no longer secured in a physical safe or in their house, but rather online in emails and documents. These digital goods are constantly vulnerable, and it is critical to warn people about how to protect them.

Two of the most popular forms of digital attacks are from Robocalls and Phishing. Robocalls are when scammers use technology to spoof caller ID numbers, appear anonymous, or mask their voice and identity to steal your valuable information. From impersonating the IRS, to disguising themselves as international banks, these calls are dangerous for the great population if encountered unknowingly. Phishing attacks are executed through forms like email and SMS messaging, and are normally activated when a victim clicks a hyperlink unknowingly. These attacks not only steal valuable information, but can go unnoticed, and can also spread from victim to victim.

Besides just these two popular forms of attacks online, the greater population is vastly under protected in terms of their online habits. From answering calls from unknown numbers, to using short and simple passwords repeatedly, the general public drives through the night of the internet without any headlights on.

Our Target Audience is adolescents and the elderly, two very different marketing groups with this unique share of being disproportionality educated on how to protect themselves online. With one in three online seniors using social media, but only 18% of all seniors feeling comfortable learning to use technology (Smith) there is a large population that needs to be taught the basic steps we will cover soon. As for adolescents, over 95% of teens have access to smartphones now, while young adults 18-24 are the most likely to be the victim of a computer virus, hacking incident or other cyber-attack (Zogby Analytics) .

These instances are most commonly taught to be protected against by a person's employer or during their schooling. The problem is that, often times financial circumstances can prevent adolescents from absorbing the information, and time places the elderly too far past the age of modern technology to informed by their employers of the risks, simply because they are already often out of the workplace.



Graph of Motivating Factors towards being targeted by an attack on the internet. The consumer based activities have risen past the school and the workplace, now targeting citizens. (PhishMe)

Why Memphis?

Memphis is a city ingrained with more than 200 years of history through its streets. Yet, from our heavy blues music found on Beale Street, to our smoky barbecue flavors just off of Central Avenue, we are modernizing the way we exist. No longer can you just find Memphians in the Tri-State area, just off of the bluff of the Mississippi. You can now find us all across the web, from our social media profiles, to our email addresses, our businesses and our personal information. All of which requires us to use precaution online, in order to protect ourselves from criminal, fraudulent, and just plain annoying activity.

So, why does Memphis need an online safety campaign? Because, in 2019, our city is beginning to step forward and innovate through the local economy, education system and transportation system, all of which will lead to increase growth. With that increase, we ought to expect more reports of Phishing attacks, Robocalls and other online scams targeted at Memphians.

Memphis is just now producing STEM-focused schools for children, and as a southern city, our job market lacks the online-focused start-ups and businesses that employ technologically educated workers. Our workforce, and overall population, is aging as a whole, and an engagement campaign to keep them up to speed on how to protect themselves is important. Last year alone, electronic extortion complaints were up by 242% (Fazzini), and Memphis was listed as the 6th most popular telephone area code (901) for a Robocall scam operation based out of Africa (WREG).

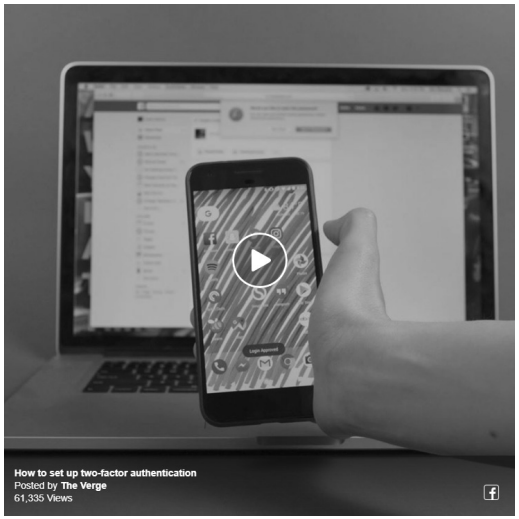
By manipulating the location and age factors in online advertising programs, such as AdSense and Facebook, we can make sure our campaign reaches the ones who need it the most— the elderly population the adolescent. Memphis's elderly population increased by 25% in just 6 years (Commercial Appeal), and as a city with only a 4 STEM academies for local students, we have an obligation to help them.

There's an apparent intersection forming in Memphis, between our culture and the internet. It can grow and be an extremely beneficial one to, as long as we protect ourselves from dangers! (MemRiverParks)

What are the Steps?

First is Education. That's the best part about this campaign having a specific focus on online advertising and social media, is that a lot of people just don't know that these type of vulnerabilities are out there and that they have them. Once it catches their attention, and they are aware of the possible side effects like identity loss and having their banking information stolen, then they often begin to take steps. From there, they can follow our campaign to stay up to date, whether it be new types of attacks across the internet, or specific ones occurring often in our local community. It's a constant feed of information that can alert new people and continue to educate them down the line.

Second is Action. Community members can start with the passive steps like being aware of incoming Caller ID tags and who they are receiving emails and SMS messages from. Small deviations in phone numbers or addresses can be purposeful and meant as a sneaky target. Also be aware of hyperlinks, especially those with long chains that seem unfamiliar.



Then, it is important to move on to the active steps such as password management and Two-Factor authentication. Community members should make passwords that are difficult to guess or crack, not like tigers123. Passwords should contain a mix of numbers, letters, special characters and capitalizations. It is also critical to not reuse a password multiple times, because once one service falls and it is obtained from it, then an attacker can access all other accounts. Lastly, Two-Factor Authentication, or 2FA, is a modern tool that requires you to confirm all logins via another port, like your cell-phone or email address. It is an incredibly useful tool to protect yourself online and can be set up on many modern online services.

The third and final step is to Spread. Just as though attacks spread from victim to victim, in order to increase the number of potential targets they can hit, we plan to spread throughout the community in order to help protect as many people as possible. This is another key benefit of focusing in on the Memphis area specifically, as we can get people communicating and spreading or engagement campaign with each other on a local basis.

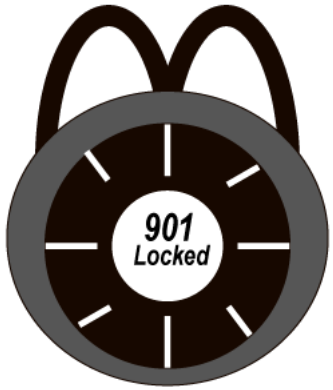
An increidbly useful video guide by The Verge on how to begin using 2FA on all of your devices, a good example of the type of content in our engagement campaign. (Natt Garun)

Important Material

Infographic

Created using Canva, it can be distributed both in print and online.

Twitter Campaign



#901Locked

Our Twitter header, engagement logo and custom social media hashtag can be used on many different platforms.

We created our hashtag with via three decisions. First, we use the city's commonly known area code 901. It instantly connects Memphis to the campaign while also providing a juxtaposition, between the wording of Locked, that makes it trendy.

Next, we use the term locked, to represent the precaution of locking down your online accounts and presence. Whether it be through passwords themselves, which a large portion of this campaign focuses on, or through the action of locking down.

Lastly, even when we aren't using the hashtag as a searchable function on social media sites like Twitter and Instagram, we are still going to be using the hashtag symbol. The slogan isn't just 901Locked, but the # is importantly engraved into it. That's because it creates an actual 10-character alpha-numeric password with capitalization differences and special characters. An unconscious and constant reminder of the need to create these complex passwords to protect ourselves.

Works Cited

Commerical Appeal. Metro Memphis' Elderly Population Growing 10 Times Faster Than Entire Region. April 12, 2018. https://www.commercialappeal.com/story/news/2018/04/12/metro-memphis-elderly-population-growing-10-times-faster-than-entire-region/498503002/

Fazzini, Kate. "Email Sextortion Scams Are on the Rise and they're Scary - Here's What To Do If You Get One. CNBC. June 17, 2019. https://www.cnbc.com/2019/06/17/email-sextortion-scams-on-the-rise-says-fbi.html

Garun, Natt. "How to Set Up Two-Factor Authentication On All Your Online Accounts." The Verge, The Verge, 27 Mar. 2019, www.theverge.com/2017/6/17/15772142/how-to-set-up-two-factor-authentication

PhishMe. "Enterprise Phishing Resiliency and Defense Report 2017". 2017. Pg. 6 https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf

Smith, Aaron. "Older Adults and Technlogy Use". Pew Research Center Internet & Technology Center. April 3, 2014

WREG. "Report Says Memphis a Hotspot for 'One Ring' Scam Robocalls. May 4, 2019. https://wreg.com/2019/05/04/flood-of-one-ring-scam-robocalls-prompts-fcc-warning/

Zickuhr, Kathryn and Madden, Mary. "Older Aadults and Internet Use". Pew Research Center Internet and Technology Center. June 6, 2012