We all know about thieves or robberies in our everyday life. But did you know that can apply to the cyber space? In America today, 89% of people between the ages of 18-29 are social media users. This was recorded by the Pew National Resource center in a 2014 survey. Due to the fact that younger people use social media on a more frequent basis and generally spend more time and rely more on the internet, young adults are more susceptible to cyber attacks and Internet fraud. In this campaign we are looking to end internet hacking by sending this message out to young adults.

According to our director of Homeland Security, “Spear phishing is the number one cause of cyberattacks, especially for young adults.” Spear phishing is where the victim receives an email from a known individual, only to find out that it was a hacker attempting to steal their personal information. For example, they could be looking for credit card information, passwords, or even bank account numbers. Just about anybody can be a “spear phisher”. Your neighbors and colleagues can steal your identity almost as easy as stealing a woman's purse, if not easier. All of your known and loved social media sites, such as facebook, instagram and twitter are all helping the DHS to spread the word about this malicious scandal. As stated on Jetscram.com’s website, with 1.32 billion people, 24.6% of all facebook users are between ages 18-29. As for Instagram users, there are 200 million users in total, 34% are between 18-29. Twitter users between ages 18-29 consume 35% of the 271 million that actively use the site. Reviewing these statistics, we have decided that most of the people falling into the grasp of spear phishing are around the 18-29 age group, so advertising on these sites is the perfect place to increase awareness. The people who prosecut these crimes are criminals with the motive to steal your personal information. But there is a simple way to stop this from happening.

The best way to prevent spear phishing is to just be smart and keep your information secure. Norton suggest if you get a suspicious e-mail asking for information, call the “friend” that sent it to you just to verify that is was them, because as stated before, these convicts will make it appear as an e-mail from one of your close contacts.

America needs to be aware of this issue within the cyberspace. Falling into one of their traps could essentially lead to the destruction of your identity and your financial stability. It is our job as The Department Of Homeland Security to protect you from these types of crimes, so we are doing our best to inform as many as possible. So, just be safe and smart and be careful of what you share.

Thanks...

-The Department of Homeland Security