Mr. President,

Each year 71 million Americans fall victim to cyber-attacks. This statistic is not just for businesses, but it also applies to ordinary citizens. The costs of these attacks are enormous and include billions of dollars in emotional and psychological damage. It is the recommendation of the Department of Homeland Security to identify these problems and inform the general public of various methods to prevent these attacks. The problems that are occurring are instigated by the operator, considering the computer simply does as the user commands. Therefore, the solution lies in addressing the weakest link: humans.

Much of the damage results from citizens unaware of what it means to “be safe” on the internet. It is crucial that the public knows how to protect themselves from potential threats. A main reason for malicious attacks is the carelessness when using certain links. A lack of adequately complex passwords can allow seemingly secure sites to be easily compromised. Also, people might not be aware of what is safe and not safe to share on sites.

To enhance cyber security, we need to make users aware of what is safe to click on and what is not. People need to know whether something is an advertisement or from an unknown site that is potentially illegitimate and unsafe. Such links should be ignored as they can damage one’s computer and, in some cases, infect it with malicious software. Not only that but clicking on unsafe links can expose private information that should be kept secure. In addition, users should create complex passwords that are not easily compromised. The passwords should be unique for each account they own. Also, password security can be improved through the use of strategies, such as biological identifiers. Furthermore, users should be cautious about what information they put on websites that are poorly encrypted. A user should always look for “https://” at the front of the site’s URL to see if their website is encrypted and secure. To make this easier for users we will direct their attention to the padlock in the address bar, which indicates this site’s safety. Therefore, websites with poor encryption can easily be hacked, and a user’s information can be exposed and used for nefarious purposes, so a person should be smart and not visit those sites.

Preventing these attacks can be easy if the general public is made aware of these threats. Through a PSA, we will use the propaganda technique of “transfer”. By doing this, we can exaggerate the characteristics of a victim and make the public of the U.S. feel negativity and disappointment towards someone who is a victim of cyber-crime. In the video, the victim is “exposing” himself to threats online by engaging in dangerous online behavior. The transfer of feeling bare and exposed is tied to these behaviors. This associates feelings of vulnerability with unsafe actions online, causing the public to not engage in said actions. Thus, internet users need to take measures to protect themselves, which will therefore neutralize the threat of cyber-attacks and damage.

PSA Video: <https://www.youtube.com/watch?v=gL0sHo51lCA>