The War for Data – A Cybersecurity Primer

# Subject/Description

As we get more and more entrenched in a digital world, cyberattacks have become more common. This is the focus of this website—what attacks have been committed, when, and the presumed *why*, all organized in various graphs on the main page, with information from the Center for Strategic and International Study’s PDF on “Significant Cyber Incidents from 2006”. Furthermore, it will also teach the ever-important *how* in order for the everyday person to defend themselves. This is accomplished with two modules: Passwords and Phishing. Passwords will explain the importance of long, unique, and ideally randomly-generated passwords for accounts, while Phishing will help people learn how to identify various social engineering attacks conducted by cybercriminals, and both of these modules will contain interactive elements to help a site visitor practice and learn. Research on this will come from well-known cybersecurity organizations, such as MITRE.

# Audience

Due to this website’s purpose, its target audience are people who do not yet know how to properly defend themselves from cyberattacks.

# Stakeholders

Along with the target audience, additional stakeholders include all that could be affected by cyberattacks, such as their employers, family, and the government.

# Deliverables

This primer will ultimately be a website with three pages: the main page (which will hold several charts for organizing and viewing cyberattack data), a passwords page (to teach a visitor of the site how to keep secure passwords), and a phishing page (to teach a visitor of the site how to recognize phishing attacks). The passwords and phishing pages will both contain interactive game-like elements, such as a ‘test the strength of your passcode’ field and a ‘identify the phishing attack’ activity.