

Week 3 Web content outline

Home Page/title- summary of site

1. This website is designed to help people understand the need for security, provide case studies, give examples, or case studies as to what has happened in the cyber security industry to make it relatable, offer a free security scan (also known as a diagnostic) and offer services to teach how to make not only your computer, but all things connected to a network secure. The website will include a FAQ section, contact us, case study, a hands-on lab, a video/research section and a section for the scans/diagnostic.

Why the need for security

2. So, the first question is naturally, WHY? Why do I need security? Have you ever, will you ever or have you ever thought about putting any sensitive information on your computer such as filling in credit card information, filing your taxes, online shopping, filling out online job applications, written something you want to later publish, inserted your full name, address, social security number, credit card number, or anything else you wouldn't want the general public to know? That alone is reason enough to want security.

Another need for security- safety

3. Now take a second and think of your car- does it have Bluetooth; can you speak wirelessly? Will it answer your calls? Does it have GPS? Can you unlock it with an app on your phone? If you have answered yes to any of the following questions, chances are your car has a network. Anything with a network can be hacked into. There have been cases **Insert case study here** where someone has hacked into a

car network and deployed airbags, pressed on the breaks, messed with the GPS, etc.... This is dangerous! You can find ways to be more secure to prevent from these kinds of attacks.

Medical security

4. How about medical devices? Anyone in your family have a pacemaker? How about an insulin pump? Any medical device that helps someone live, and has anything wireless? If you said yes to any of these ask yourself: Is my loved one's life worth the risk, or the peace of mind in knowing they are secure and alive. There have been reports of people hacking into insulin pumps and either stopping the insulin, or causing the patient to OD, through remote access of the pump. How about stopping a pacemaker and putting malware that will kill the battery in less than 3 days?

Consequences/wrap up of why security

5. Security issues are everywhere, at the gas station, with our cars, credit cards, passports, phones, tablets, headphones, computers, and so much more! Cyber security is the next nuclear war, it's the modern terrorism. You can do something about it! You can try and prevent the problem rather than clean up the mess. You can brace yourself and those you love. So why security? Because you love. You love yourself, your family, and your friends. You stay secure because you love your identity and want to keep it. You up your security because you know what could happen if you don't.

Different types of cyber breaches

6. Security threats are everywhere. In your car, medical devices, phones, tablets, computers, home security systems, anywhere there is technology, there is potential for a threat. It could be a virus, malware, or a worm. So, what are each of these?

What is a Virus VS. Worm VS. Malware?

7. A virus is defined as, “a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data” whereas malware is defined as “software that is intended to damage or disable computers and computer systems” and a worm is defined as “In a computer, a worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.”

Intro to fAQ

8. For my website, there are a few things I want to incorporate, one is a FAQ section, below I will write some of the questions I will answer, knowing what questions to ask is the hard part so I will answer them later.

- Who can I speak to for more information?
- What are some things I can do in the meantime to be more secure?
- Where are you located?
- When can I expect to hear back?
- How can I guarantee satisfaction?
- Who can be affected by security vulnerabilities?
- What are some things I should look out for?

- What should I do if I think my security has been compromised?
- And How do I know how to set good passwords?
- These are just a few questions that will be found in my FAQ section.

Find My Threats

9. In addition to a “Why Security” section, I want to have a “How to find security threats” section, which will include a free security scan, as well as a Pro version security scan which will actually scan your operating system and not just the files on your hard drive. So, this section will include the scans, and a lot of information as to what things could be a virus. This section will include text, links to the scan (and a link to pay if you buy the pro version) and video tutorials. This section is designed to teach you how to find the security threats.

Where to start

10. I also want to incorporate a “What can I do now?” section. This section will include things like, how to make good, safe passwords. How to set up MFA on applicable site and why MFA is more secure. It will also include things such as what to look for in a malicious email, basic safety precautions (like not putting a lot of sensitive data on Facebook or other social media), and different options of software (obviously including my own software) that can be purchased to help constantly scan your computer. I will include why you want it scanned regularly. I personally will have an update weekly to be more secure so I will advertise that. This comparison of software will be in the format of a chart; therefore, it will be easy to read and designed great.

