Cyber Security Essentials – Planning Document

To Research;

Core Components:

* ISO 27001

A security standard provides requirments for an information security management system (ISMS)

<https://www.iso.org/isoiec-27001-information-security.html>

* Cyber Security Essentials

Partially covered in Wednesday lesson. Section below with extra info. This is the best choice for the presentation as it links with the security module we’re doing.

* Amazon Web Services

I've used this before, however some extra research into the proper setup of an AWS server would be a good plan.

45 minute face to face training event.

Would be a very good plan to research presentation methods, communication styles, dialogue types, etc.

On top of this, it'd be good to think up different techniques for different group sizes and the positives/negatives for each style.

Key points:

* Outline impacts of security risks
* Explain and show types of security risks and what can result
* For example, XSS and SQL injection
* Social engineering
* Malware
* Talk about methods of being safe from social engineering, basic security practises, evaluation of risk.

<45 minute presentation: explanation, verbal exercises, interactive exercises, group tasks, video.

|  |  |  |
| --- | --- | --- |
| Timestamp | Component | Specifics |
| 00:00 | Introduction | Quick introduction to the presentation, the reasons behind it such as safety and security in the business, as well as outlining what will be coming up in the presentation |
| 03:00 | Description of impacts of cybersecurity risks | An explanation of what security risks and attacks can mean for an individual, such as impacting their social standing or their balance, as well as impacts on a business, including denial of service, loss of money and trust, damage of equipment or loss of life. Introduce examples that outline historical losses that a company has faced because of a cybersecurity issue. |
| 10:00 | Video involving tips that can be applied by anyone. | YouTube. (2018). World-famous hacker offers his top cybersecurity tips. [online] Available at: https://www.youtube.com/watch?v=NCSQU\_58WbU [Accessed 3 Oct. 2019]. - Approx 6:30 long. |
| 16:30 | Lead onto what specifically can be done | Possibly an interactive experience? Ask groups what they think can be done regarding cybersecurity, to protect both themselves and the company they work at. Add onto the list if there’s something important missing, i.e. encryption, password security, avoiding utilising unknown electronics like USB drives. |
| 25:00 | Explain some well known cases of social engineering and the impacts they had | Social media ‘hacks’ involving 2 factor authentication being used as an attack vector; having information about someone and pretending to be them allows for you to get a copy of their sim, potentially giving you full access to things like email accounts. Linus Tech Tips as an example |
| 30:00 | Video from Linus Tech Tips regarding 2FA hack. | <https://www.youtube.com/watch?v=LlcAHkjbARs>  (Don’t use the complete video: timestamps 3:00 -> 7:06) |
| 34:00 | Reiterate points covered about what individuals can do | Mostly as a conclusion, expect that there’ll be 5 or so minutes of delays across the whole presentation. Use this time at the end to reiterate points, explain potential impact, tell some jokes. |