**Lesson 31 – Computer Safety and Ethics Research and Share**

|  |  |
| --- | --- |
| **Work Stations** | **Research your answers. Report to the class. Use the Presentation and your computer. Write in the space provided. You can also draw and write on the back of this paper.**  **Explain Your Thinking! / “In your own words explain . . .”** |
| **Group 1** | In what ways can you help to maintain a safe computing environment? (p.5) |
| **Group 2** | What is OSHA and what purpose do they serve? (*www.osha.gov)* |
| **Group 3** | What is “ergonomics” and why is it important? How can you avoid computer related injuries? What is RSI? (p. 6 and elsewhere) |
| **Group 4** | Discuss the security risks found on slides 7, 8, and 9. (networks, hacking, data loss) |
| **Group 5** | Discuss the security risks found on slides 10, 11, and 12. (software threats) |
| **Group 6** | What are ACCESS RESTICTIONS and how are they employed? (p. 13) |
| **Group 7** | What is WORKPLACE PRIVACY? What computer privacy do typical employees enjoy? (p. 14)  What is a NETWORK USAGE POLICY? |
| **Group 8** | What is meant by a SECURE website? How would you know if a site is SECURE? (p.15 & elsewhere) Type and example of a secure website. |
| **Group 9** | Explain the following terms and how they are used: TLS and SSL (p. 16) |
| **Group 10** | What is PHISHING? Explain an example of a PHISHING SCHEME. (p. 17 and elsewhere) |
| **Group 11** | What are COOKIES? What is SPYWARE? What is the best way to secure your data? (p.18 & elsewhere) |
| **Group 12** | Define the following terms: browser hijacking, brute force attacks, hacking, hardware firewall |
| **Group 13** | Define the following terms: keylogger, private key, public key, sniffer |
| **Group 14** | How do you create a strong password? What elements would you include? What would you avoid doing? |