Tool Kit / Resources

Target Audience: *Small/Medium-size Business and Non-Profits*

1. **How do you prevent being a victim of cyber-crime/attacks? Best practices for cyber hygiene.**
   - Develop and implement IT protocols (acceptable use policies) for your company that all staff review and sign that lists out what is allowed/not allowed, etc.
   - Basic protocol/tips:
     - Implement strong password management procedures
     - Require regular software updates and implement a software management process
     - Provide cybersecurity awareness training to your employees about different types of phishing attempts and other cyber attacks
     - Define proper usage of USB devices and other mobile devices
     - Restrict downloading/uploading programs/software/apps to authorized personnel
     - Provide basic operational guidelines (turn off computers at the end of the day, ensure that all sensitive information is secured (paper stored in locked file cabinets, electronic information is encrypted, etc.)

2. **How do you prepare in case a cyber incident occurs? What information do you need?**
   - Develop a cyber incident plan for your organization/business (resource: SANS free templates) that includes plans/processes for actionable step that will be taken if an incident should occur.
   - What types of information/documentation should you keep/gather in advance of an incident? And be sure to update regularly:
     - What information will you need to know about your network? (i.e. keep an inventory of current hardware & configurations, including software and version numbers, maintain a current network architecture diagram showing how the devices are connected in your network, etc.)

3. **If an intrusion or incident occurs, what do you do next?**
   - Refer to your company's cyber incident plan and take immediate steps to limit impact to business/organization that will allow you to continue to be operational
   - Report the incident to the authorities (FBI) and engage a forensic IT expert if necessary
   - What immediate steps do you need to take
     - Disconnect the computer from the network:
     - If possible, do not shutdown the computer (important information may be stored in memory)
     - Do not send emails from the compromised device
     - Document what occurred pre/during/post the incident

4. **Who can help if an incident occurs?**
   - Refer to the Cyber Defense 101 Contact and Resource Sheet