Professional IT Services
Serving the entire West Sound, Sequim, and Surrounding Areas

# Annual Information Security Awareness Training

(2 hours)

---

**Overview:**

Are your employees aware of their role in protecting company data? In response to the recent work from home model many of us are adopting, we have seen an uptick in the amount of threats and attacks cyber criminals have been launching against end users. Now more than ever is an incredibly important time to make sure your staff is aware of their role in protecting your company's data.

This class will equip you and your staff with the knowledge and skills needed to face the constantly changing cyber threats and, more importantly, discuss how to avoid and respond to them. This training also fulfills the PCI and HIPAA compliance requirement to conduct an annual Cybersecurity Awareness training.

This training can be taught in your office, or via video conference. For a video conference, we can record the training session and provide it to you and your team for offline viewing if some of your staff is unable to attend virtually. We can also split this class into two, one hour sessions to more easily fit employee's busy schedules.

NOTE: Because cyber security is constantly evolving, we recommend this training be taught annually to your team, as ongoing employee education is imperative to company security.

**Price:**
Please call for a quote.

**Registration:**
Call our office to register for a class, discuss pricing, or ask for more information. Registration is required for all classes, must be done at least 24 hours in advance, and is on a first-come, first-served basis.

**Agenda:**
See next page for a detailed outline of course content.

**Course Agenda:**

1. Malware
    a. Types of Malware
    b. Malware Behavior
    c. Delivery of Viruses
    d. How to Prevent and Respond to Infections
2. Social Engineering
    a. Vishing and Phone Scams
    b. Phishing and email scams
    c. Social Engineering Prevention and response
3. Passwords and Account Security
    a. What makes a good password
    b. Password management
    c. Alternatives to passwords
    d. Multi factor Authentication
    e. Password Culture and Strategies
4. Safe Internet Habits
    a. What not to click on while browsing the web
    b. Identifying bad URL's
    c. Browser security settings and plugins
    d. Verifying downloads and scanning for malware
5. Physical Security
    a. Clean Desk Policies
    b. Contractors and Vendors
    c. Office Visits
    d. Public Networks
6. Miscellaneous
    a. Backups
    b. Encryption
    c. Cloud Security
7. Q&A