

Digital Security Awareness and Prevention

Oregon Small Business Community

BUSINESS EMAIL COMPROMISE

- Carefully scrutinize all e-mail requests for wire transfers, be suspicious of requests for secrecy or urgency.
- Confirm wire transfer instructions with requester, especially when the requester is out of the office. Use an alternate and previously established communication avenue, such as a phone call.
- Require multiple approval authorities, and establish this procedure in such a way that would be difficult for fraudsters to discover.
- Register all company domains that are slightly different than the actual company domain.
- These same precautions should be taken for any requests for W-2 records or other sensitive information.

POINT OF SALE (POS) MALWARE

- Employ Application Whitelisting to restrict PoS system to intended uses.
- Update and regularly patch the PoS Operating System and Applications.
- Limit internal access to the physical PoS Device.
- Disallow remote access, or install two-factor authentication if remote access is used for servicing. Avoid relying only on password logins.
- Employ End-to-End Encryption, this can be costly but is effective.

DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)

- Establish and maintain an effective partnership with your network service provider to quickly enable implementation of upstream mitigation strategies during an attack.
- Consider also establishing relationships with companies who offer DDoS mitigation services. At a minimum, identify companies who provide this service so you know who to contact if needed.
- An extortion demand may be received with the threat of DDoS attack. Contact law enforcement if your business is extorted by cyber criminals.

RANSOMWARE

- Regularly update and patch software, and set anti-virus and anti-malware solutions to auto-update.
- Maintain principle of least privilege, no user should be assigned administrator access unless absolutely needed.
- Backups are critical, have secure backups offline and regularly test your backup restore procedures.

Small businesses should consider developing an incident response plan with a checklist of actions to be taken if the company is a victim of a cybercrime such as the ones listed above. Train your employees to be aware of the threats and the response procedures.