SEL Computer Security Steps

Summary of a Webinar presentation for Idaho Commerce by Frank Harrill, SEL on 8-11-20

Example

Small businesses have become top targets for online theft of information and funds.

Example:
An Idaho contractor who was doing business as usual. A customer they had recently completed a significant job for and invoiced was contacted by a third party impersonating the contractor. The email asked the customer to deposit the payment for the invoice into a Wells Fargo bank account. The customer tried to do this but received a warning message so did not proceed. The contractor was contacted for verification and told the customer they did not have a Wells Fargo bank account. They then discovered their computer had been hacked. Ransom, extortion, skimming, spying, and outright theft are common.

Security First Principals

1. Rapid Incident Response. A plan in place to respond quickly to mitigate damage.
2. User Education and Testing because most breaches begin with a phishing email.
3. Multifactor Authentication
4. Risk-based timely patching

Considerations

1. Look in to insurance coverage.
2. Back-up your important data.
3. Never use the same password for more than one site and consider a password manager such as Last Pass https://www.lastpass.com/ or Kee Pass: https://keepass.info/
4. Create a procedure in your company that requires second party verification for a payment change that is not by email or text.
5. Test your security and rate your risk with a company such as https://webscan.upguard.com/ , https://www.bitsight.com/ , FICO Cyber Risk Score: https://www.fico.com/en/products/cyber-risk-score , or: https://securityscorecard.com/
6. To find out more: https://www.cisecurity.org/controls/cis-controls-list/
   Bonus: To find out about the NIST controls needed for some government contracting: https://www.nist.gov/cyberframework

Revised: 01/20/21 BL