PROTECTING YOUR BUSINESS FROM CYBER ATTACKS

Develop a Culture of Security

- Culture of Security Starts at the Top
- Provide Training for Employees AND Their Families
- Learn Red Flags of Phishing Emails
- Keep Current on Common Scams
- Review Business Processes: “Do We Do Things This Way for Security or Convenience?”
- Keep Anti-Virus, Operating Systems, and Hardware Patched and Updated (Automatically if Possible)
- Don’t Use the Same Password Everywhere; Use a Password Manager App for Added Security
- Limit Details in Social Media Posts (Don’t Accept Friend Requests from Friends You Already Have)
- Review Social Media Security Settings Regularly
- Don’t Wire Money to Someone You Don’t Know

Reporting Scams:

- Justice Department Resource Page https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime
- FBI Internet Crime Complaint Center (IC3) https://www.ic3.gov
- FBI Phone - 1-800-CALL-FBI
- FTC Consumer Protection – https://www.ftc.gov
- FTC Identity Theft Reporting https://identitytheft.gov

Training Resources:

- KnowBe4 - www.KnowBe4.com - blog.knowbe4.com
- KnowBe4 Free Training - www.knowbe4.com/homecourse Password is: homecourse
- (1 hour course designed to help your family make wise decisions online)
- Free 240 page “Cyberheist” eBook - https://info.knowbe4.com/free-e-book
- (Includes a form to subscribe to their weekly “CyberheistNews” newsletter)
- Cyberwire’s free “Hacking Humans” podcast, sponsored by KnowBe4
- Compromised much? - https://haveibeenpwned.com

THANK YOU FOR ATTENDING!

BIG CREEK
“Growing Redwoods for the Future”