Cybersecurity Awareness Training

Creating Your Culture of Awareness

Most cyberattacks start with human error. Someone clicks on a link or sends money based on an email they believe is from a reliable source. Phishing is, after all, the most common method of attack today.

Layers of Learning

So how do you create this culture of awareness? A strong training program has many layers of tools. First, start with an assessment and videos to educate everyone about the threat that is out there and how they can avoid it. Follow up with monthly newsletters, quick games and security infographics.

Test Your Employees

Cyber threats change constantly and phishing simulations ensure your employees keep “in the know” on the latest threats. A phishing campaign sends emails bi-monthly to check if your employees would click. The fake email can be an offer from a retailer, or a message from a bank. Will they click? At the beginning of training, many do! But as they get better at recognizing scam emails, the numbers fall and you have a workforce trained to recognize and report suspicious behavior.

Training Topics

- Email Security
- Human Firewall
- Incident Reporting
- Internet Use
- Mobile Devices
- Passwords and Authentication
- Privacy
- Security Awareness
- Social Media
- Wi-Fi Usage
- Ransomware
- Remote Work
- Spear Phishing
- Vishing

JigsawTek | P.844.544.7638 | info@jigsawtek.com | www.jigsawtek.com