Tips on Creating a Culture of Security Awareness
INTRODUCTION

How do you motivate your employees to help strengthen your IT security? How do you get your workforce to buy into the importance of a security awareness culture? Without motivation, most employees don’t think about security, which means it’s difficult to fully leverage the power of your people against security threats.

Here are 7 important tips on how to get a culture of security awareness (and constant security vigilance) started in your workplace.

“Developing a security awareness program isn’t a destination, but a journey.”
#1 FOCUS ON THE BASICS OF SECURITY

The hassle-free and easy-to-understand concepts of security are the ones that people embrace quickly. Lead with security steps such as two-factor (or multi-factor) authentication, best password practices, password managers, and keeping software and firmware updated. Make security as approachable as possible and emphasize it as an ongoing effort, not a one-time thing.
#2 INVEST IN EMPLOYEE SECURITY AWARENESS TRAINING

Good security awareness training breaks up training into units that address individual security topics and provides ongoing training. Annual training modules, periodic tests, newsletters, and email tips that teach security awareness in fun, creative, or engaging chunks can help keep security top-of-mind for your employees.
#3 MAKE SECURITY PERSONAL AND VALUABLE

Security shouldn’t be presented as an obstacle, but rather as a way for employees to bring value to your organization. Emphasizing that proper security procedures and behavior improves the operation of the company is more useful than scare tactics.

Orient your security awareness campaigns towards your staff’s and organization’s goals and values. Speak one-on-one with your staff members to convey the personal importance of security rules and processes. Educate employees about how they can cause serious damage to their organization through non-compliant or inattentive behavior. Conversely, they can improve the company by being aware and security-conscious.
#4 TRY THE TOP DOWN APPROACH

Make sure your directors, management team, and supervisors are leading the charge for security awareness and driving the initiative. People at the top set the tone and drive cultural changes. A cybersecurity team alone can’t be responsible for changing culture if the business leaders don’t embody security values too.

Additionally, it isn’t just a single group that should be responsible for creating a culture of security. Multiple departments, from Marketing to HR and Legal to Finance, have a role to play in spreading the word and measuring the effectiveness of your security initiative.
#5 REWARD EMPLOYEES FOR SPEAKING UP

Give your employees an incentive to stay watchful and speak up when they notice suspicious emails or activities. Gamify practicing good security habits to create a little healthy security competition in the workplace.

Positive rewards encourage behavior. Consider doing a prize drawing for every suspicious email employees report. An incentive and good reward may be taking the time to thank a user who reports a suspicious email, speaking personally to users who have demonstrated particularly good security habits, or publicly recognizing people.
#6 HELP AT-HOME WORKERS AND TELECOMMUTING EMPLOYEES TO WORK SAFELY

Employees can now work from anywhere - the local coffee shop, hotels, airports, and home offices. Encourage these employees to trust and communicate with the security team and management to ensure they’re not taking risks with client data, work files, equipment, and more. Help employees get set up with virtual private networks (VPNs) and educate them on additional steps to reduce the potential for attacks, threats, and data loss. Just because someone isn’t in the office shouldn’t mean that they’re left out of the loop on security practices.
#7 RUN SIMULATED PHISHING ATTACKS AND SHARE THE STATISTICS

Run regular phishing attack simulations in your organization to help your staff learn to recognize and deal appropriately with suspicious and malicious emails.

What is a simulated phishing attack? Using a security service, you can send a fake phishing email campaign to your staff. If anyone is “caught” by the fake attack, you’ll see who it was. Let your staff know who was caught (did one department or office do better than another?), who wasn’t, and who properly reported the phishing attack to supervisors and/or the security team.
WHERE TO NEXT?

Creating a cyber security culture is the responsibility of every manager and employee to prevent against a breach or attack. Engaged team members who receive ongoing awareness training and regular communication foster a strong cyber security culture.

Do you need help tackling any of these tips? We can help your business in these efforts with our free IT Security Awareness Training, Ongoing Education, Simulated Phishing Attacks, Security Reviews, and Assessments.

Keep cyber security top of mind and contact us! Reach us by email at hello@oxen.tech, on our security website at security.oxen.tech, or by phone at 888.296.3619.
TIPS ON CREATING A CULTURE OF SECURITY AWARENESS

SOURCES


https://www.tripwire.com/state-of-security/security-awareness/3-tips-on-how-to-create-a-cyber-security-culture-at-work/

https://securityintelligence.com/top-five-tips-for-creating-a-culture-of-security-awareness-at-work/

http://www.huffingtonpost.ca/matthew-held/cyber-security-work-b_16578830.html

"Creating a Culture of Awareness”. StaySafeOnline.org.  
https://staysafeonline.org/re-cyber/creating-a-culture-of-awareness/