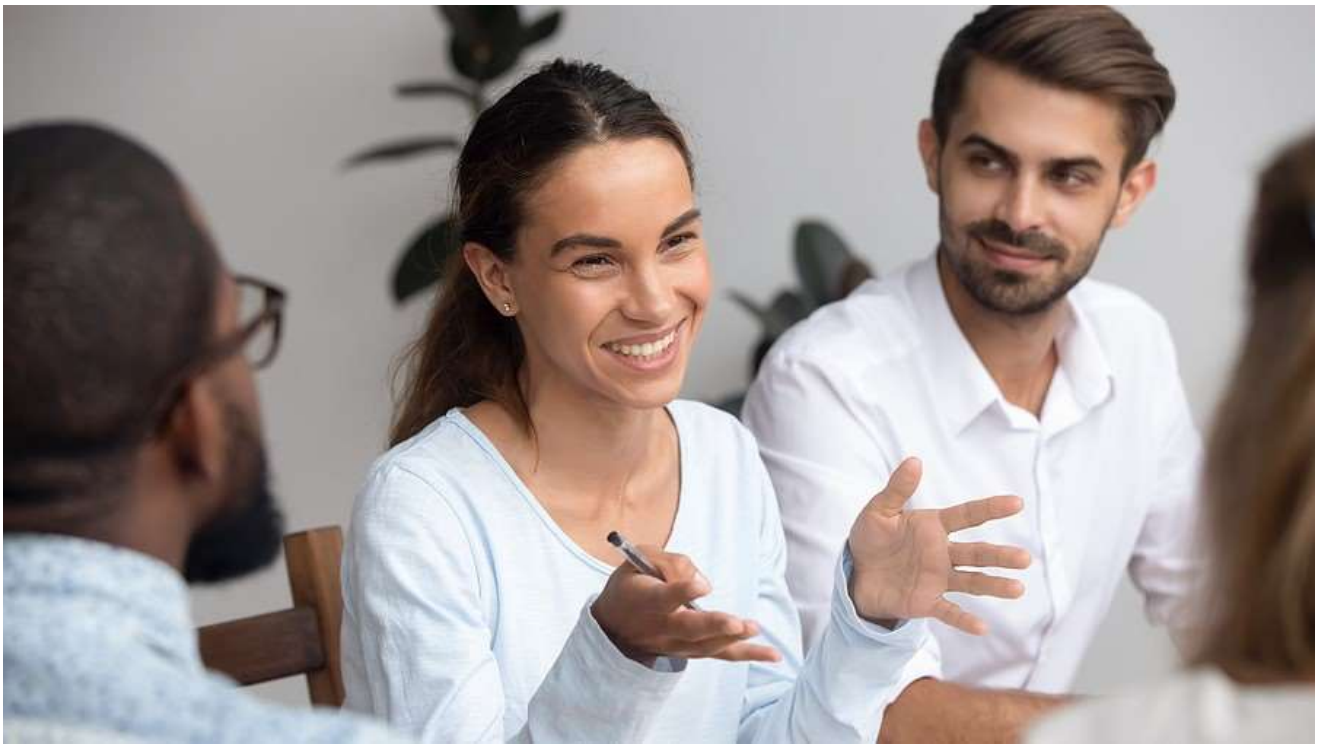
Tips to Engage End Users in the Cyber Security Discussion



Employees unintentionally create security problems by using bad passwords, clicking phishing links, mishandling sensitive data, and disregarding other rules of basic data protection. Training employees properly and engaging them in the cyber security discussion could save your organization millions of dollars in data breach recovery costs.

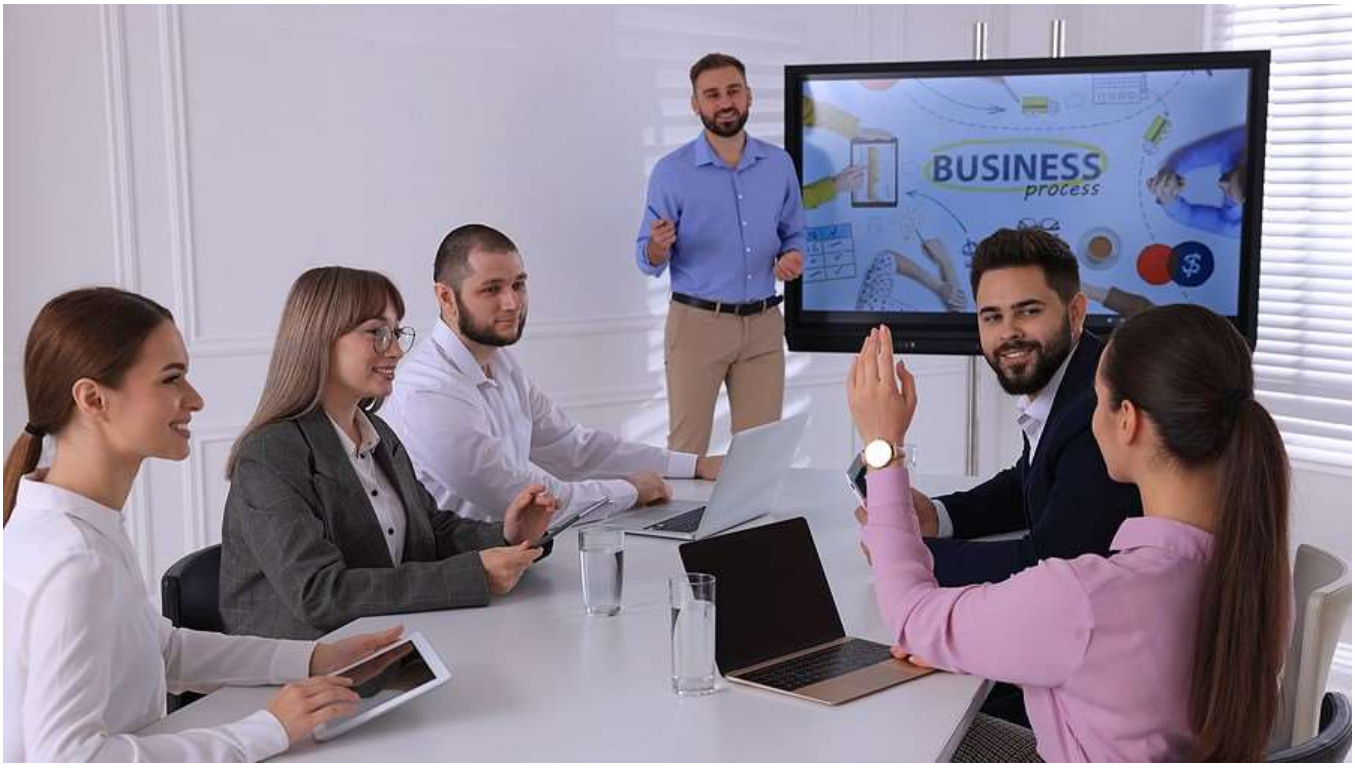
Many security awareness training programs fail. If employees who attend by constraint find the information uninteresting, they pay little attention. Hence, they fail to apply the training when they encounter real-life cyber security threats. It's far better to engage end users in a cyber security discussion where they participate and learn to see themselves as part of the solution.

When presenters use interactive training techniques, learners absorb the material more readily. For example, discussing a real-life scenario that employees might encounter in their daily work pulls them in. To make the training interesting, positive, and hands-on, employ these cyber security discussion tips that draw on research into effective training strategies.

Make Cyber Security Discussion Groups Small

For effective cyber security training, security experts suggest small groups or one-on-one meetings. Use them to identify and build realistic threat scenarios that employees relate to. For example, ask participants to draft a spear-phishing email using information about the company they know.

Small groups encourage greater participation. Once they have identified several possible threat scenarios, get them talking about how to respond to such threats. Their ideas provide valuable input to improve the risk profile of the company.



Make the Discussion Interactive

Unless you are an amazing presenter, your discussion group will lose interest quickly when you are the only one talking. Involving participants in the discussion is a proven way to keep their attention. Short, interactive training modules also keep users engaged and increase retention.

Ask questions to assess the level of understanding or invite them to ask questions. Solicit opinions about proposed policies and procedures. Invite participants to be part of the solution as much as possible. Engage learners at all levels of the organization with an interactive discussion.

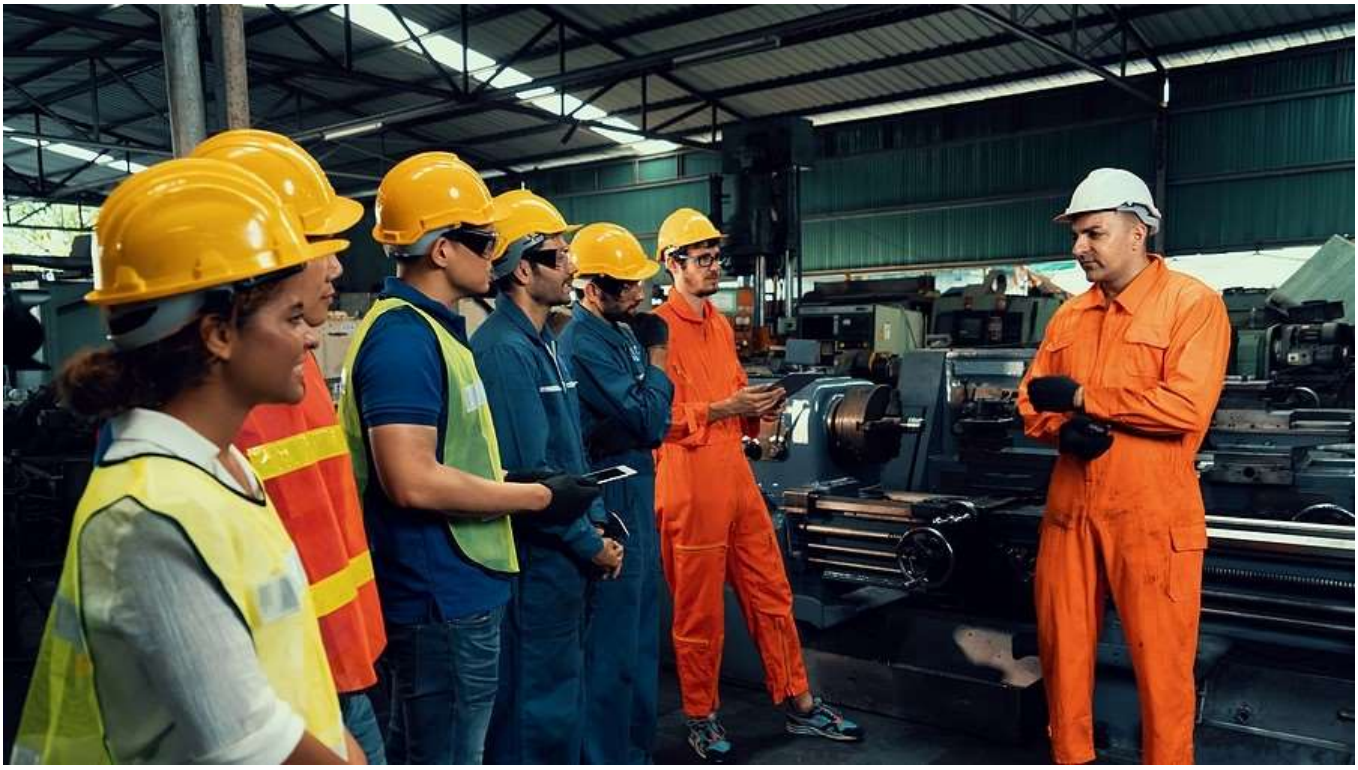
Use Technology, Simulations and Games

When used in the discussion sparingly, technology and videos help to get participants interested in the topic. For example, once users learn about compliance requirements and the dangers and signs of a phishing attack, they need to practice what they have learned.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year

Simulated phishing campaigns provide that opportunity in a controlled environment. When users click on an attachment or link in a simulated phishing email, they receive just-in-time training. Phishing simulations also identify the employees who most need the training.

Almost everyone likes playing games. It's a timeless method to stimulate learners' thoughts and engage them in the topic. In groups where employees want to stand out and excel, competitive games activate participants' energy and best thinking.



Relate the Cyber Security Discussion to Employees' Role and Access

A marketing executive faces different security threats than a machine operator on the shop floor. For example, the marketing VP may become the target of a spear-phishing campaign. Factory workers, on the other hand, need to understand how to recognize IoT cyber security threats to the Internet-connected machinery they operate.

When the discussion reflects the learner's job duties and level of network access, it provides relevant, useful information. Because they can easily see how it relates to their daily activities, this type of discussion engages learners more fully.

Emphasize the Why

When employees understand the rationale behind security rules, they become more likely to follow them. Why should I care about email safety and access procedures? Because the damage from a cyber-attack could sink the company, costing you your job. And to be effective, everyone in the company who touches data must share the responsibility for cyber-security.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 500 | 500 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year

Make sure employees know how to recognize potential threats. Then give them the tools to counter those threats and teach them how to use them. They represent the first line of defense, and they need to know what they face and why their diligence makes a difference.

Encourage Outside Learning

Don't give the group everything. Encourage them to do some of their own research on appropriate topics. For example, you could ask them to look up recent cyber security breaches and report on the ones they found most relevant to your company.

Prepare something for each discussion to add a bit of a problem-solving. Using unknowns and investigation increases the engagement of the group. For example, ask group members to track how many phishing emails they receive in a week.

Deliver Enterprise-Grade Phishing Awareness Training

To help organizations get the most out of their cyber security discussion, eMazzanti offers targeted security awareness training. MXINSPECT uses an approach designed to engage employees and change behavior. Targeted, just-in-time training and phishing simulations teach users how to recognize and respond to phishing attacks.

2015 | 2013 | 2012 Microsoft Partner of the Year
WatchGuard 5x WatchGuard Partner of the Year
Inc. 5000 | 5000 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010
hp Partner of the Year
ShoreTel Sky Partner of the Year