CUSTOMIZING END USER CYBERSECURITY EDUCATION FOR YOUR COMMUNITY AND CULTURE

Ensuring the cybersecurity of your community depends as much on end user education as it does policies and technology. A layered security strategy for local governments and school districts must include a thoughtful end user cybersecurity awareness and education program that includes components such as phishing exercises and other cybersecurity training programs.

TAKE-ACTION TIPS

JUST GET STARTED
Not doing anything at all is the worst thing you can do. Even if you do not have the policies, you can get started on training. A great place to start is by evaluating your biggest Risks and training for those.

WHO DOESN'T LIKE FREE STUFF?
Freebies are fantastic! Do a web search, as many training and awareness vendors offer free basic versions of their more sophisticated products and services. There is lots of variety in content and activities to get and keep employees’ attention so that they learn how to protect themselves and your organization.

DON'T USE PHISHING AS A 'GOTCHA!'
Phishing simulations are a great way to spread awareness of suspicious links and attachments. Just make sure you are not using them in a way that causes intimidation or fear. Start by sending a baseline phish to the whole organization without telling every single person what you are doing (inform the help desk and HR). Keep it moderate in difficulty THEN communicate like crazy about the click rate!

TIP: It is okay, and often extremely effective to use humor and keep exercises light hearted. Remember, it’s training! Keep it positive and reward people who report both simulated and real phish.
REMEMBER: YOU ARE NOT HR!
Treat your program as training. When employees repeat offend, give them a chance to understand the policy. It is important to establish a partnership with HR, but not to become HR. Remember, we are in the business of protecting people; we are not here to fire people or restrict their ability to do their jobs.

DO YOUR RESEARCH
Look at multiple vendors before choosing the one right for you. Your choice will depend on the culture of your organization, as well as the style you are looking for. Do the research and then validate it with a testimony from a trusted peer before moving forward.

KEEP IT FRESH
Remember that you are competing for attention with everything in people's lives, from their own job duties to what they are making for dinner tonight! Keep your training engaging, short, and customized. There are many new and innovative ways to make things personalized to your organization, department, and individual employees. Create an experience that makes them come back for more! And PLEASE stop with the one hour a year presentation. Quick, weekly content is a smarter choice.

THE END GOAL= CULTURE CHANGE
If you keep your eyes on culture change, then you will find the right tools and your organization will be better off. Try to create an environment where everyone feels they have a role to play.

ADDITIONAL RESOURCES

- Cybersecurity Collaborative: Home Page
  [https://www.cyberleadersunite.com](https://www.cyberleadersunite.com)

- The National Association of Counties: Cyber Security Priorities and Best Practices

- National Cyber Security Alliance: Cybersecurity Awareness Month Champion Program

- National Cybersecurity Center: “Text-to-Learn” Cybersecurity Awareness Training