HipLink®

10 Questions to Help Nail Your Cybersecurity Awareness Campaign

Trusted SINCE 1995

www.hiplink.com

1. What's Fundamental?

If you've ever been an employee, you've probably sat through meetings about policies that someone (not you, of course) forgot about as soon as the meeting ended. How do you make sure employees retain what they hear, especially when the information in question is as crucial as the security of your network?

First and foremost, make sure that your awareness campaign helps employees understand the most critical pieces of the policy and its rationale first rather than burying them in extra information.

2. What's Important and Relevant to Which Audience?

Cybersecurity experts understand why CXOs are targeted so often for phishing attacks. They have high levels of access and, often, low exposure to practices that might inoculate them to social engineering. Likewise, different situations will be more relevant to staff in different geographic areas or in different roles.

Relevance makes ideas sticky. Talk to employees about security issues they're likely to encounter at work in their specific roles. They'll be more likely to remember and more likely to change relevant behaviors.

After all, why run campaigns that don't impact behavior?

3. Where and When do Staff See Campaign Messaging?

When someone sees a reminder at the time and place they need it, they are far more likely to remember without a reminder later on.

Make sure staff see aligned messaging often and in multiple places to make sure it sticks. But don't just throw signs everywhere. Where do companies place signs to effectively remind people to turn off lights? By the switch.

4. How Can You Involve Key Leadership?

When employees see leadership as participants in your campaign, instead of just as mouthpieces, they'll remember better and be more likely to follow suit.

Feature key staff in videos, and let them demonstrate key practices. The more human they become to the rest of the organization, the more real the campaign's goals and practices will feel.

5. Is That a Myth?

Sometimes in organizations, watercooler subcultures develop that pay lip service to threats. To combat this tendency, make sure you're focusing on facts and using clear, relevant examples.

For cybersecurity campaigns, consider high-profile breaches from the previous year that are relevant to your industry like these examples. Did your company see a breach? Use it.

6. What Does Your Campaign LOOK Like?

Between 70 and 90% of the information that the average person remembers is visual. Show, don't tell! Providing clear visual cues tied to different levels or types of threats will help people in your organization remember threats and identify their seriousness.

Similarly, we provide children visual cues in class in order to help them think about their behavior. Have you flown on an airplane? Think about the style and clarity of the images on effective instruction cards.

7. Does it Appeal to Staff Self Interest?

If anything teaches better than an example, it's a story or example that involves personal stakes and consequences.

On one hand, your campaign can show staff how to manage relevant security practices outside of work. For example: How do you handle your phone in public that might put you at risk? How and why are children targets for hackers?

On the other hand, helping employees connect their behavior to consequences for themselves and their coworkers can also carry a lot of emotional weight.

8. Is Our Messaging Memorable?

Think of awareness campaign messaging as marketing.

Short, memorable headlines stick. Ever heard the saying "loose lips sink ships?"

Storytelling is a tactic that smart awareness campaign builders use to help audiences remember key messages. Remember the boy who cried wolf?

9. Why?

Most people, if they understand the purpose behind a program, will buy in if they can. Don't be afraid to talk about the bottom line, your company reputation, and the trust your customers place in your business.

'

Especially if you're making big changes to support your cybersecurity efforts, make sure staff understand what's happening and the reason for it before you alter their work lives. They'll trust you more if you do.

10. Is it S.M.A.R.T?

As Peter Drucker famously told the business world, "What gets measured gets managed."

Before you even develop the messaging for your cybersecurity campaign, determine what metrics you will use to know that it has been effective. What will be different after implementation than before? How will you quantify those changes?

Setting S.M.A.R.T (Specific, Measurable, Attainable, Realistic, Time-bound) goals to help you measure the impact of the campaign (and systematizing measurement as you go) will go a long way to helping you take steps that matter and make adjustments if they're needed.