Becoming Cybermindful

A Toolkit for Developing Cybersecurity Awareness at Your Organization

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE

This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

Why Cybermindfulness Matters

If you're reading this, you already know your organization is at risk from cybercrime—the proof is all over the news.

When data breaches happen, it's rarely because technical teams fell asleep at the wheel and failed to put safeguards in place. More often, someone within the organization makes a completely human error when a convincing phishing ploy hits their inbox. Unfortunately, there's no firewall for the human brain to protect us from the glitches of attention and judgement that allow social engineering schemes to succeed. So, what's an organization to do?

Many of us have tried the "annual training" model as a defense against social engineering. You know the drill: Once a year, employees are asked to watch a few videos, provide the right answers to an online comprehension quiz, and promise not to click on anything bad. This might be helpful if a security incident has us looking for someone to take the blame, but checking the box on training doesn't really help our colleagues prepare for daily battle in the arena of their inbox and web browser. Cybersecurity is a war, not a battle, and our troops need regular practice and encouragement if we expect them to be on guard day after day—not just on training day.

We also know that cybersecurity isn't always our community's favorite topic. Often our users are checked-out, believing they're too insignificant a target. Or they're demoralized by the mountain of data breaches announced in the news, and believe if a hacker wants their stuff, they're going to get it—so why bother? Neither belief inspires engagement and action. We need an approach to cybersecurity training that meets our users where they are and invites them to join the resistance.

We need an approach to cybersecurity training that meets our users where they are and invites them to join the resistance.

In the pages that follow, we'll explain how to help your users embrace the middle ground between carelessness and hopelessness: Cybermindfulness. Promoting Cybermindfulness at your organization will encourage users to have a right-sized awareness of cybersecurity risks, a sense of agency about their own role in protecting themselves and your organization, and the ability to take appropriate action in the face of threats (or mistakes—because we're all going to make them).

Read on to start Becoming Cybermindful

What is Cybermindfulness?

We know what you're thinking. "Cybermindfulness? You just made that up." Well, yes. But for good reason.

Here's the deal. It's hard to change our habits. We all know that good habits don't happen overnight. And we also know that unless we've got something motivating us, we're likely to keep on doing what we've been doing instead of what we should be doing.

That's why traditional "one-and-done" cybersecurity education approaches don't really work. After sitting through a four-hour workshop or clicking through an online training module learning about the scary, costly threats facing my company, sure I'll think twice about what I'm clicking on once I'm back at my desk ... for a few days. But, our human nature requires reminders and motivation along the way to keep us moving in the right direction. That's where the Cybermindfulness comes in.

Cybermindfulness promotes three components our workforce needs to defeat social engineering: Awareness, Agency, and Action.

Awareness

Awareness is exactly what you'd expect—knowing what the risks are in our digital lives, both at work and at home, and their consequences. Awareness is what lets us say, "I get it. Ransomware, Spear Phishing, Business Email Compromise are all schemes cybercriminals are likely to throw our way. And when they happen, it's going to be an expensive hassle." But just because we know better doesn't mean we'll do better (that third bowl of chips and queso isn't gonna feel good later, but it's so hard to resist ...). That's where Agency comes in.

Agency

Agency is feeling up to the task. If our users have agency, they've got both a sense of ownership ("I have a role to play in keeping my organization's information safe!") and confidence ("I can identify and avoid phishing ploys! And if I mess up, I know who to call!"). This personal efficacy is central to the whole Cybermindfulness thing. If our users don't believe their actions will make a difference, it doesn't matter if they can define every social engineering tactic in the book to earn their Certificate of Completion in the annual training. With agency, we're ready to act.

Our workforce needs three components to defeat social engineering: awareness, agency, and action.

Action

Action is about doing the right things at the right time to keep our info assets secure. Action enompasses all those tactical things we want our users to remember: don't reuse passwords, recognize a phishing message, report suspicious activity promptly, and so on. There are a million specific ways to enhance our computing security. Most important, though, is simply for our users to keep their antennae up when they're online. Then, when that social engineering ploy shows up, however it shows up, they'll catch it … and hopefully report it, too!

Awareness, Agency, and Action connect (not unlike the distinct but coordinating pieces of Optimus Prime) to compose Cybermindfulness, the Zen-like understanding that, while there are a whole lot of threats out there, we each have a role to play.

A role that's not too technical, is well within my abilities, and has a meaningful impact on the health of my organization. And I'm ready to act accordingly when the moment arrives.

Simply put, Cybermindfulness gives our user community permission not to be experts, but makes sure they know that engaged "not-experts" are an irreplaceable part of our cybersecurity team.

We each have a role to play in keeping our organization healthy and strong.

Why Cybermindfulness Works

So, why does this approach work?

Social science research around communication and behavior change has directed our path, particularly the handful of theories summarized on the right.

With these observations about the mind in mind, the Cybermindfulness model pays particular attention to:

Inviting Relationships

Communication theory tells us the messenger is as important as the message. Our users are going to pay more attention to messaging from a source they know, trust and like; sounding and acting like the empathetic humans we are goes a long way in helping our users really hear what we're trying to say.

Providing Friendly Expertise

The key word here is "friendly." Hopefully our users already think our IT department is technically competent. But they also need to know we're here to help them. If users have questions or make a mistake, we want them to feel comfortable reaching out to our IT staff without fear of judgement or blame.

Blending the Personal and Professional

Many of our colleagues don't have a trusted source of info when it comes to cybersecurity. With home routers, online banking, and kids at home on the internet, they're looking for help keeping themselves and their family safe. Teaching them smart habits for their personal computing lives builds the habits they need to stay safe at work, too.

Providing Tools and Practice

We want to bake in the good habits we're advocating by both arming our colleagues with the information they need to make smart choices around their use of tech *and* providing regular opportunities to test their skills, for instance, through monthly phishing exercises. Practice won't make perfect, but it sure will increase confidence, aptitude, and a sense of self-efficacy.

Behavioral Theories Guiding the Cybermindfulness Model

Communication Theory
Communication is a stochastic process. Messages comprise both content and context. Fear appeals have limited usefulness.

Diffusion of Innovations
Acceptance of new ideas is strongly influenced by our interaction with organizational opinion leaders.

Elaboration Likelihood
Humans are cognitive "misers"; we use peripheral processing (heuristics and "rules of thumb") to process more information.

Health Belief Model
Behaviors change when we feel the risk AND have a sense of agency and efficacy.

Cognitive Response Theory
The more consistent our cognitive responses are with a message, the more influential the message will be.

Inoculation Theory
People can be assisted in their efforts to resist the persuasive efforts of others by practicing defensive strategies.

See References on page 9.

Rewarding Interaction

Positive reinforcement can be a powerful tool for cementing new habits. Rewards can be tangible like pens, mugs or other swag as a prize for engaging in a training activity or reporting a suspicious email. And—bonus!—physical stuff that's likely to stay out in the open can also serve as an ongoing reminder of Cybermindfulness. But don't underestimate the power of intangible rewards like a sincere word of thanks in a personal email or a congratulatory shout-out in a monthly e-newsletter.

Committing to the Long Haul

Habits don't change overnight and a culture of Cybermindfulness won't happen after one email or mandatory training session. Plan on keeping on with it—regular messaging, friendly responses to questions, ongoing gratitude for participation and reporting. Wash, rinse, repeat.

Social science applied to real, live communication techniques. That's where the magic happens.

Reinforce your community's good habits with a genuine and sincere *thank you*.

Guiding Your Organization Towards Cybermindfulness

If you're planning to roll out a Cybermindfulness initiative at your organization (and we hope you do!), we'd recommend you incorporate all of the following elements.

But don't worry—we've provided some resources to make reaching out to your users as easy as possible, even if your time is limited.

The Buy-In

Before you put your user community on the road to Cybermindfulness, be sure to engage your leadership. Take time to explain that building a community of early alert allies within your staff will help protect your organization from cyberattacks. If your senior leaders aren't on board with the program, chances are slim that you'll be able to effectively build a Cybermindful culture.

The Launch

Chances are, regular messaging around safe computing topics will be new to your organization, so kick it off right! A message from a senior leader of your organization, whether that's the CEO, CIO, president, or principal, expressing their support and setting the stage will help grab your colleagues' attention. The message should explain the "why" and the "WIIFM" ("what's in it for me?") of Becoming Cybermindful, announce what the organization should expect over the coming months, and build excitement.

The Messaging

This is the meat (or tofu, if you'd prefer) of the program. The Cybermindfulness toolkit includes 12 monthly newsletters you can send to your user community. Remember, repetition and reinforcement are key to keeping our Cybermindfulness synapses firing, so commit to sticking with a full year of outreach!

The Practice

A particularly effective way of building agency, the "Yes, I can!" confidence that helps motivate action, is having a chance to practice a new skill. One of the best methods for strengthening Cybermindfulness muscles is through phishing simulation exercises. Consider adding a monthly phishing component to your organization's education efforts, if budget and time allows. Check out our phishing resource guide for ideas on how to get this rolling at your organization.

The Proof

If you're going to bother doing all this, you're going to want to know it's making a difference. One way to figure this out is by conducting a brief survey at the beginning and end of each year of messaging. We've provided a survey resource guide you can use to more easily assess your organization's development of awareness, agency, and action. You can also gather useful feedback from help desk reports. For instance, are your users reporting more suspicious emails? That's a good sign their Cybermindfulness antennae are primed to detect social engineering.

The Follow-Through

And after you've done all that? You're going to want to keep the conversation going. When you've made it through a year, think about how you can continue to provide ongoing nuggets of information to keep Cybermindfulness front of mind with your team. You might be able to reduce the frequency of your messaging, but you'll want to keep the lines of communication open so your users know where to go when they have questions—or something suspicious to report.

WRAP UP

Some Things to Keep in Mind

You know your organization best.

Your organization's culture will determine what's likely to play best with your users.

You can create messages tailored to your audience.

Don't be afraid to adjust message length or add or omit topics based on what you know your team might find most interesting and engaging.

You're a human talking to other humans.

Non-jargony language, direct address (referring to your users as "you" rather than "employees" in messaging), and talking informally can help you connect more authentically with your colleagues.

You're allowed to have fun with it.

Cybersecurity is a serious threat, no doubt. But that doesn't mean we have to terrify everyone. In fact, social science research suggests that inspiring fear might even undermine your messaging (Witte & Allen, 2000). Don't be afraid to reassure your folks with some humor or throw in some off-topic content periodically to keep them on their toes.

You're not going to catch everyone.

Despite your best efforts, not everyone is going to pay attention, not everyone is going to embrace their inner Cybermindful mind, not everyone is going to care about cybersecurity. That's ok. Think of it like herd immunity—the more folks we have looking out for signs of trouble, the better. Even if that's not everyone.

University of Dayton
Center for Cybersecurity & Data Intelligence
937-229-1929
udaytoncyber@udayton.edu

Find more tools at go.udayton.edu/cybersecurity

References

Becker, M. H. (1974). The Health Belief Model and personal health behavior. *Health Education Monographs*, 2, 324–508.

Greenwald, A. (1968). Cognitive learning, cognitive response to persuasion. In A. G. Greenwald, T. C. Brock, & T. M. Ostrom (Eds.), *Psychological foundations of attitudes* (pp. 147–170). Academic Press.

Ng, B. & Xu, Y. (January, 2007). Studying Users' Computer Security Behavior Using the Health Belief Model. A paper presented at the Pacific Asia Conference on Information Systems, Auckland, New Zealand.

O'Keefe, D. J. (2013). The elaboration likelihood model. In J. P. Dillard & L. Shen (Eds.), *The Sage handbook of persuasion: Developments in theory and practice* (2nd ed., pp. 137–149). Sage Publications.

Pfau M., Semmler S. M., Deatrick L., Mason A., Nisbett G., Lane L., et al. (2009). Nuances about the role and impact of affect in inoculation. *Communication Monographs*, 76, 73–98.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Witte, K. & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, 27, 591–615.