The Realist's Guide to Cybersecurity Awareness

TIPS FOR ENGAGING AND EMPOWERING EMPLOYEES IN THE REAL WORLD

Barkly™

Introduction

Raising awareness and training employees on cybersecurity is hard. It's draining. It's thankless. And all too often, it's ineffective. A big part of the problem is that we approach it with unrealistic expectations, and with tactics and messaging that may resonate with us, but not our audience. As a result, there's often a disconnect between our security-minded priorities and those of the rest of the company.

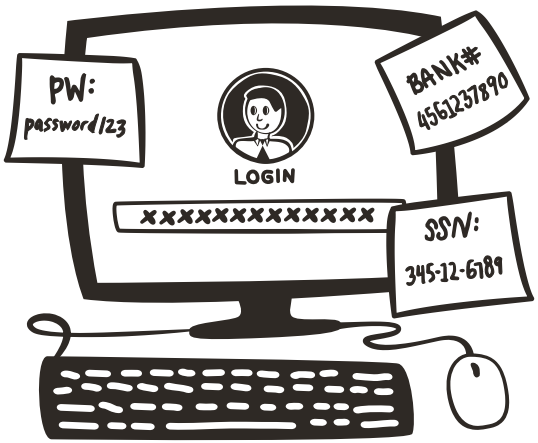
In an ideal world, we'd be recognized by management and co-workers as the esteemed guardians of information and sage-like purveyors of critical know-how we clearly are.

The reality is a little bit different.

The following tips will help you close the gap.

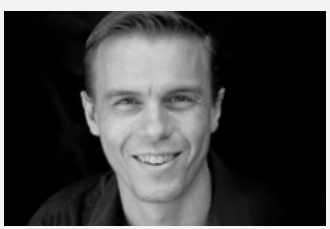
WE WANT TO BELIEVE...

Not only are employees eager to create strong, unique passwords, they're also able to easily remember them, and even make it a point to update them regularly!



BUT, IN REALITY...

You get passwords like “12345” and “password.”



TROY HUNT
Microsoft MVP for Developer Security,
Pluralsight author, and international speaker

troyhunt.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

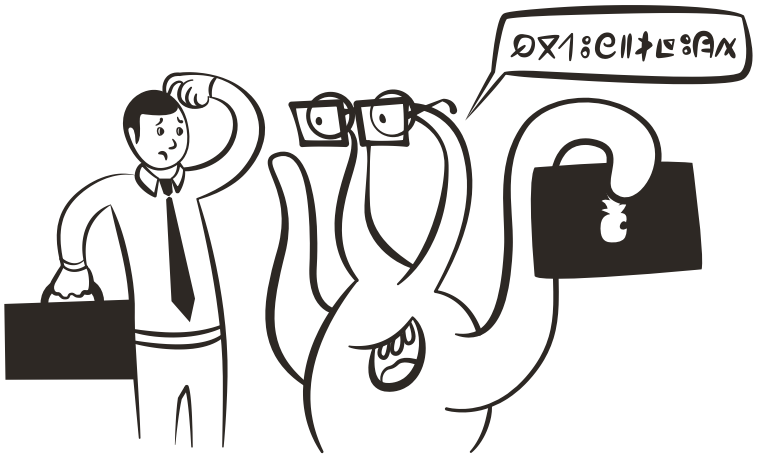
“Explain that password managers are our friends.”

Strong, unique passwords are a necessity, but by that very definition they’re not memorable. Passwords managers are the answer as they allow you to create one strong, unique password (which we can memorize), which protects and encrypted collection of other strong, unique passwords (which we can’t memorize en mass).

Tweet this

WE WANT TO BELIEVE...

We speak the same language.



BUT, IN REALITY...

We may as well be speaking Blorg.

COREY NACHREINER
CTO, WatchGuard

watchguardsecuritycenter.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"When it comes to your messaging, simplify, clarify, repeat."

Training is not about making end-users InfoSec experts. It's about sharing just enough information to foster some key behaviors. In other words, if you are training them about buffer overflows flaws, you're doing it wrong. Instead, you should be training them on how to recognize phishing emails or how to interact with unsolicited attachments. In the end, you want them to know enough about the potential problem that they will adopt the right behavior.

Don't spout acronyms without explanation. In short, don't speak in the same shorthand you use with peers. Even if you think a term or acronym is well recognized, spend the extra minute to explain it. Source: Dark Reading

Tweet this

WE WANT TO BELIEVE...

Name-dropping those big, scary data breaches in the headlines will hit home.

BUT, IN REALITY...

No one really cares because it happened to someone else.

JOHN N. STEWART
SVP, Chief Security & Trust Officer at Cisco

cisco.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"This time, make it personal."

You can have a little fun with cybersecurity. I like to make these things personal. That means I've taken examples of employees where they've gotten themselves into an upside-down situation because they double-clicked this, installed that or whatever, and they just become the voice and go, "You know what, guess what I didn't realize until today."

They'll make videos, they'll give quotes, they'll write a blog, laugh with us. That makes it personal because it was a friend, it was a colleague. It was something that happened at Cisco, not something that happened somewhere else.

Source: Wall Street Journal

Tweet this

WE WANT TO BELIEVE...

Security is one of every employee's top priorities

BUT, IN REALITY...

They've got jobs to do.

LYSA MYERS
Security Researcher at ESET

welivesecurity.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"Connect the dots between security and their existing goals & priorities."

When we're working in our capacity as security advocates – or just as people trying to convince others to do something we think would be beneficial – determining what "beneficial" means to our audience should be step one before presenting our suggestions.

There are people out there whose most important goals are along the lines of "responding quickly in an emergency," "raising employee morale," or "the free flow of information." These goals are not necessarily contradictory to security, but it may seem so if these concerns are not specifically addressed in our educational pleas. Source: Dark Reading

Tweet this

WE WANT TO BELIEVE...

Everybody will do what's right; our people and the people and organizations we partner with, too.

BUT, IN REALITY...

"Right" has too many meanings. Sometimes "right" is about safer, but often it's about cheaper, easier, or faster.

JACK DANAHY
Co-founder and CTO at Barkly

barkly.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"Make explicit the behaviors you want to see and the practices you expect people to adhere to."

We tend to have an artificial and incorrect predilection that everyone holds the same beliefs and priorities as we do. If we highly value our customers' security, we assume that all our employees and our partners will value it to the same degree.

That's not always the case, but we shouldn't judge too harshly when others don't yet understand or prioritize security. Instead, we need to be up front with them, explain our security choices, and repeatedly outline what we expect from them. Employees and partners will certainly skew to doing what's right, but they are much more likely to succeed when we consistently help them understand what that means.

Tweet this

WE WANT TO BELIEVE...

We can knock out security awareness with one-and-done computer-based training (CBT).

BUT, IN REALITY...

Effective training requires consistent reinforcement and exposure to real-world scenarios.

CHRISTOPHER HADNAGY
CEO Social-Engineer, Inc.
social-engineer.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"Consider CBT just one of many tools in your tool box."

If you wanted to learn how to box you would go to a boxing gym. The trainer would set you up with protective gear and then tell you how to deliver a punch and take a punch. You would never step into the ring unprotected till you were ready.

Can you imagine if you walked into the gym and the trainer sat you down and showed you a 20 minute CBT then said, "Okay, you ready?" Of course not, that's ridiculous.

Well, your people are entering the ring right now, and they have never stepped into the ring and they are not ready or prepared. We encourage each company to have realistic phishing tests that show what it is like to get phished (take the punch) and how to report it properly (give the punch). CBT's have their place as part of training but they will not fix the problem.

Tweet this

WE WANT TO BELIEVE...

Hitting users with mock phishing attacks can always scare them straight.

BUT, IN REALITY...

Employees can sometimes feel like you are tricking them instead of teaching them.

AMY BAKER
VP of Marketing at
Wombat Security Technologies

wombatsecurity.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"Quickly move the focus from 'what you did wrong' to 'how we can get better.'"

No one likes to feel fooled. When it comes to mock attacks and penetration tests, make sure to communicate your plans a few weeks in advance so that you don't ruin your phishing tests and follow up with users right away. Right after telling them they made a mistake, use a constructive message that encourages them to view the exercise as a positive learning experience rather than a failed test or a gotcha. Then provide more in-depth training so that they have the knowledge to avoid the next attack.

Tweet this

WE WANT TO BELIEVE...

We can force employees to be more security-minded.

BUT, IN REALITY...

We're just as likely to make them floss.

MASHA SEDOVA
Senior Director of Trust Engagement
at Salesforce

trust.salesforce.com

EXPERT REALIST SAYS TRY THIS, INSTEAD:

"Encourage employees to actually opt into security initiatives by introducing gamification principles."

This is what we call discretionary performance – getting people to want to do security instead of [feeling like] they have to. The way we do that is by including elements like gamification, positive incentives, rewards, and recognition to get people to understand these are behaviors we would like to see them do, and actually reward people when they demonstrate them, as opposed to just punishing bad behavior.

A key component of a successful security awareness program is making our employees actually get their hands a little bit dirty with the things we're asking them to do. Plus, we all like to get a "thank you" or a high-five for good behavior, and that is something that's irrelevant of the type of company you work for or the size. Source: FEDcyber 2014

Tweet this

At Barkly, we're realists, too. We understand security can be complicated. That's why we're building a simple solution designed to safeguard your company with strong endpoint protection that's fast, affordable, and easy-to-use.

Share this guide with your favorite fellow IT realist on Twitter

SHARE

STAY INFORMED! SUBSCRIBE TO THE BARKLY BLOG:
blog.barkly.com