They say “it takes one to know one.” After 15 years in the information security industry, I have to agree. Even though I have spent my career focused on helping organizations design, develop and implement security awareness programs, I still mishandle my passwords, click on links I shouldn’t and am far too trusting in general. What can I say, I am an early adopter, I believe in the Internet as the great provider and I want instant access to information. So, for all of you out there who have made the same mistakes I have, we are in this together.

Security awareness is mostly about common sense, but like other security precautions, it’s easy to let down your guard. I browse the Web, check email, use mobile devices and share information countless times a day. With all that connectivity, it’s hard to stay vigilant and very easy to cop an “I’m just going around the corner” attitude. But where the car reminds me to put my seatbelt on, I don’t have a warning tone on my laptop reminding me not to click a link.

Reminding others to do the right thing never makes you popular either. No one wants to be “that guy.” Even worse, there are those people who remind you that wearing a seatbelt will not guarantee your safety. This is the information security equivalent to telling you that companies get breached even though they have security awareness programs. So what does all this mean? Should you give up on seatbelts and security awareness?

Well, would you disable the seatbelt buzzer on your car? Safety precautions never come with guarantees, but individuals and businesses still practice safety every day. Creating a culture of security awareness is just one of the many things you must do to protect your assets. Employees, entry-level and experienced, are spending more and more time interacting and exchanging information electronically at work and at home. Aiming your staff with the skills to practice safe Internet usage is good for them, and good for your organization. It is common sense.

**How Do I Stay On Top of It?**

Vulnerabilities appear in your environment every day. For example, everyone wants to use their tablet or smart phone to conduct business. And it makes sense: phones are portable, powerful and connected. Then there are the “put it in the cloud” chants, which also make sense, as the cloud is everywhere making information always accessible. New technology equals new threats. Which leads to the purchase of more technology to protect that technology.

And the cycle continues. You are exposed to new threats every day. Foreign hackers are perched at their screens around the clock probing your defenses. They are organized, highly skilled and well-funded. Staying ahead of these threats takes effort but, just like vulnerabilities, all too often we don’t focus enough on the human aspects. A recent survey at BlackHat 2012 revealed that “unwitting employees” are the highest security concern of information security professionals.

Helping your organization stay ahead does take effort. But remember, it “takes one to know one.” You need to think like the bad guys. What are the assets that are valuable? How would you go after them? Learning about common attack methods and commonly attacked assets makes you realize that hackers know that the way to valuable data is through the people that handle the data. Read the technology section of your daily paper, subscribe to security blog sites, rely on your partners and peers, and use common sense.

**How Do I Convince Others to Pay Attention?**

You have to commit to being “that guy.” Planning and implementing security awareness programs will not make you popular. But the key question to ask everyone is: can we afford the risk? Data breaches are more than just embarrassing. Service interruption, fines and incremental costs associated with the breach, loss of customers, and permanent brand damage can be very hard to overcome. Do everything you can to prevent a breach, starting with your people. Make your security posture about more than process and technology.

A Ponemon Survey conducted in 2012 found that “negligent insiders are the highest ranking threat to an organization’s payment data.” This survey data is backed by Trustwave’s forensics experience and extensive analysis of more than two million business passwords. The Trustwave 2012 Global Security Report states that the most common password global businesses use is “Password1.” The bad guys make a point of preying on weak credentials: 80% of breaches are the result of compromised administrator accounts because we make it easy for them to log in.

The most common corporate password is **Password1** because it just barely meets the minimum complexity requirements of active directory for length, capitalization and numerical figures.
What Should I Teach Them?

Don’t overwhelm staff with security awareness training that is irrelevant to them. Not everyone has the same exposure to sensitive and private information. Focus on the people that are exposed to this information and arm them with best practice behaviors to minimize the risk that they become a source of a leak. Help them understand the behavior that makes them more vulnerable to attacks. Teach staff what they need to know in their everyday work and use language they understand.

Content and courses often include examples of the latest viruses, phishing ploys and social engineering scams. Examples are only good as long as they are examples and not intended to present an exhaustive list of what to watch for. Provide staff with the skills to recognize all threats by teaching them the characteristics of a threat, and how their behaviors can open them up to risks and vulnerabilities.

Teach them skills that will help them recognize tomorrow’s threat. Teach them that the stakes are high. Teach them that their actions can play an active role in reducing risks and even preventing an incident. Teach you staff “how to fish” not just how to avoid a specific phish.

In many respects the difference in approach is the difference between training and education. Training is an event that teaches specific skills and behaviors. Education is about laying a foundation of knowledge that will lead to future insight, and will get your staff involved with mitigating future risks. Institute security awareness education not just security awareness training.

Having a partner can really help here, especially a partner that is involved on a daily basis with tracking security threats and vulnerabilities.

If I Build It, Will They Come?

Breaches happen every day around the world. Breaches cost money. Breaches have the potential to expose private information to misuse. Don’t let your staff become complacent about these concerns. Insist that they stay vigilant.

Security awareness education is not an option. It should be mandatory and ubiquitous, and include both short and long term learning outcomes. Measure completion and administer testing if you are serious about transferring skills to everyday tasks. Let people know they are being measured. Have consequences or incentives that motivate people to comply. We may not agree that observation of speed limits should be mandated or that you should be fined for not buckling up, but recognize that compliance enforcement is not about individual rights but a matter of public safety. Fines and penalties increase adherence, so consider using them.

Online learning delivery methods provide the advantage of automatic completion tracking. And since all learning management systems (LMS) provide the advantage of automated tracking and reporting, there are simple ways to provide auditable evidence of completion. Make print brochures readily available and ask managers to ensure they are read and applied to the workplace.

But don’t rely on just your learning management system. Use as many delivery methods as you can to support the program. This means potentially providing online training, classroom training, email reminders, posters, mentoring and access to daily information security news. If staff cannot access online learning, then use print. The adage the something is better than nothing applies here. Print-based programs don’t have the advantage of automated tracking and reporting, but there are simple ways to make print brochures readily available and ask managers to ensure they are read and applied to the workplace.

Make security awareness learning inevitable by ingrasing it in the workplace. Add security awareness to your new hire training, reinforce it through online learning and leverage existing events to reinforce the security awareness program.

Remember, if you want them to pay attention, make sure you and your management do as well. Lead by example and complete the training. It takes one to know one! Make your boss complete the training and make your boss’s boss complete the training. Then share progress results with everyone. This level of transparency will help build trust with your staff as well as show that the program is important.

Making your program universal reinforces the notion that security is everyone’s responsibility. Whether you are a cashier at a grocery chain, a store manager, a corporate accountant, a customer support specialist or the CEO, you play a role in securing sensitive information. We should all take that responsibility seriously and do their part to learn how to protect this information and the people we serve.

27% of IT organizations have top executives or privileged users who have fallen for malicious email attacks.

What are you going to do?

Users trained in avoiding phishing and scam emails fell for these malicious emails 42% less than those without training.

27% of IT organizations have top executives or privileged users who have fallen for malicious email attacks.

What Should I Teach Them?

Don’t overwhelm staff with security awareness training that is irrelevant to them. Not everyone has the same exposure to sensitive and private information. Focus on the people that are exposed to this information and arm them with best practice behaviors to minimize the risk that they become a source of a leak. Help them understand the behavior that makes them more vulnerable to attacks. Teach staff what they need to know in their everyday work and use language they understand.

Content and courses often include examples of the latest viruses, phishing ploys and social engineering scams. Examples are only good as long as they are examples and not intended to present an exhaustive list of what to watch for. Provide staff with the skills to recognize all threats by teaching them the characteristics of a threat, and how their behaviors can open them up to risks and vulnerabilities.

Teach them skills that will help them recognize tomorrow’s threat. Teach them that the stakes are high. Teach them that their actions can play an active role in reducing risks and even preventing an incident. Teach you staff “how to fish” not just how to avoid a specific phish.

In many respects the difference in approach is the difference between training and education. Training is an event that teaches specific skills and behaviors. Education is about laying a foundation of knowledge that will lead to future insight, and will get your staff involved with mitigating future risks. Institute security awareness education not just security awareness training.

Having a partner can really help here, especially a partner that is involved on a daily basis with tracking security threats and vulnerabilities.

If I Build It, Will They Come?

Breaches happen every day around the world. Breaches cost money. Breaches have the potential to expose private information to misuse. Don’t let your staff become complacent about these concerns. Insist that they stay vigilant.

Security awareness education is not an option. It should be mandatory and ubiquitous, and include both short and long term learning outcomes. Measure completion and administer testing if you are serious about transferring skills to everyday tasks. Let people know they are being measured. Have consequences or incentives that motivate people to comply. We may not agree that observation of speed limits should be mandated or that you should be fined for not buckling up, but recognize that compliance enforcement is not about individual rights but a matter of public safety. Fines and penalties increase adherence, so consider using them.

Online learning delivery methods provide the advantage of automatic completion tracking. And since all learning management systems (LMS) provide the advantage of automated tracking and reporting, there are simple ways to provide auditable evidence of completion. Make print brochures readily available and ask managers to ensure they are read and applied to the workplace.

But don’t rely on just your learning management system. Use as many delivery methods as you can to support the program. This means potentially providing online training, classroom training, email reminders, posters, mentoring and access to daily information security news. If staff cannot access online learning, then use print. The adage the something is better than nothing applies here. Print-based programs don’t have the advantage of automated tracking and reporting, but there are simple ways to make print brochures readily available and ask managers to ensure they are read and applied to the workplace.

Make security awareness learning inevitable by ingrasing it in the workplace. Add security awareness to your new hire training, reinforce it through online learning and leverage existing events to reinforce the security awareness program.

Remember, if you want them to pay attention, make sure you and your management do as well. Lead by example and complete the training. It takes one to know one! Make your boss complete the training and make your boss’s boss complete the training. Then share progress results with everyone. This level of transparency will help build trust with your staff as well as show that the program is important.

Making your program universal reinforces the notion that security is everyone’s responsibility. Whether you are a cashier at a grocery chain, a store manager, a corporate accountant, a customer support specialist or the CEO, you play a role in securing sensitive information. We should all take that responsibility seriously and do their part to learn how to protect this information and the people we serve.

About Roy Lamond, M.Ed.

Roy has spent the last 15 years in the security industry being “that guy.”

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today’s challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations--ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers--manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit https://www.trustwave.com.