Security Awareness Program –Email Templates



# Executive Summary

This documents provides drafts of different types of communications that you may use in the coordination, deploying, maintaining or measuring of your security awareness program.

# Advisory Board Announcement

If you plan on forming an Advisory Board to help you plan and maintain your security awareness program, you will most likely need to send out an email to the organization asking for volunteers. Here is an example of such an email.

*Folks,*

*We are looking for volunteers who would like to get involved in and help improve our organization’s cyber security program. You do not need any technical background or any experience in security, just a desire to learn and help. In fact, the less security experience you have, the better. We are forming a new committee called the Security Awareness Advisory Board. The purpose of the group is to have individuals from throughout the organization provide feedback on how we can better help people secure themselves in their daily activities, both at work and at home. Plan on this position taking about four hours of your time per quarter, as you help review and provide feedback on various cyber security projects we are developing. Not only does the Advisory Board give you the opportunity to meet people from throughout the organization and help secure our information, but what you learn will make you a more aware and secure person at home. Executive Director So-and-So will be heading this committee.*

*If you are interested in learning more or becoming involved, please contact [Your Contact Information Here].*

# Initial Kick-Off Email

This is an example of an initial kick-off email that would announce a new or updated security awareness program. We highly recommend that a senior executive send out the email. While this example uses email as the modality of communication, you can have the senior executive post via an internal blog, taped interview, podcast or whatever works best for your organization.

*Team,*

*As you know, we take information security extremely seriously. To help ensure all of you understand our security expectations, and what you can do to help protect not only yourself but our organization, we will be kicking off a permanent security awareness program that all employees and contractors will be required to take.  This training covers a variety of topics that apply not to just work but also home, including how to secure your family.  In addition we will be providing materials throughout the year to keep you updated.  Finally, we will be testing your understanding of this training, to include quizzes, awareness surveys and assessments. Expect an email in the first week of October providing you your login for the online awareness training.  You are then required to complete it by the end of October. This is mandatory training.  And in case you were wondering, yes, I will be participating in the same program. Please take it seriously and apply what you learn.  I look forward to seeing the results.*

*If you have any questions about this program or suggestions on how to improve it, please contact [Your Contact Information Here]. He is overall responsible for our security awareness program and will be happy to hear from you.*

**NOTE**: If you have some type of internal security awareness portal or website, you may want to reference that in this email so people know where to go for additional security awareness materials.

# Online Training Account

This is an example email that your LMS can send to your employees and staff giving them their initial login and password information for their online training.

*Dear $$firstname$$*

*As you know, in our organization information security is an extremely important matter. We take various steps to protect both you and the organization. One of these steps is to provide security awareness training to all staff. As such, we have created an account for you on our security awareness portal. Your current login information is:*

*username: $$username$$*

*password: $$password$$*

*(you will have to change your password when you login for the first time)*

*To start your awareness training, login at*

*$$url$$*

*Please cut and paste the address into the address line at the top of your web browser window. All staff is required to complete the training by the end of October. The training consists of ## videos, each about 3 minutes long. Most of the content applies not only to our organization, but protecting yourself and your family. In fact one of the videos is on how to protect your kids. All total the videos and quizzes come to about one hour. If you do not have time to finish the training in one sitting, you can log out and then log back in at a later time. The system will remember where you left off. If you have any questions or problems with the online training, please contact [Email Here].*

*Thanks!*

*[Signature Block]*

**NOTE**: If you have some type of internal security awareness portal or website, you may want to reference that in this email so people know where to go for additional security awareness materials.

# Reminder Email

Your LMS should support the option to send out a reminder email. People will forget to take the training, you should follow-up with reminders one to two weeks after the account emails go out.

*Dear $$firstname$$*

*This is a friendly reminder that you need to complete your online security awareness training by the end of the month. As you may remember we have created an account for you on our security awareness portal. Your current login information is:*

*username: $$username$$*

*password: $$password$$*

*(you will have to change your password when you login for the first time)*

*To complete the training, please login at*

*$$url$$*

*If you have any questions or problems with the online training, please contact the [Email Here].*

# Training Completion Email

Once you have deployed your training and users have taken the online training, you may want to take the opportunity to get their feedback via a survey. One option is to send out a survey every six months, then use that to improve your program. If possible, once again have the CEO send out this request, demonstrating your organization’s commitment to security. Or perhaps have this as an automated email generated by the LMS after the training is complete.

*Team,*

*Thank you so much for taking an active part in our security awareness program. So far almost everyone has taken the training. We hope you found this valuable. We know and understand that security is a continuous process, we can never stop improving. As such, we would greatly appreciate if you could take five minutes of your time and complete the following security awareness survey. We are asking you what you liked best about the training so far, but also what you feel what needs to be improved. Finally, we are hoping for suggestions on how we can make this program more useful.*

**NOTE**: You may want to consider offering a prize randomly awarded to people who complete the survey. If you do offer a prize, you will find one ‘big’ prize will get a better response then lots of ‘small’ prizes. In other words, you will most likely get more responses if there is ONE iPad offered as a prize, as opposed to TEN free lunches offered.

# Phishing Simulation Announcement

If you plan on having a phishing simulation program, we highly recommend you let people know about it ahead of time. Let them know what the ground rules, what they should and expect and why. Clear communications ahead of time are key for people accepting the program.

*Folks,*

*As you know, we take information security extremely seriously. As part of our ongoing security awareness training we will be kicking of a phishing simulation program. A phishing simulation is nothing more than when we send out a phishing email pretending to be a cyber attacker. We will be simulating the very same email attacks that the bad guys are constantly sending. However, these simulations will not harm you in any way, they are only designed to help you learn how to identify these scams and protect yourself at work and at home. A couple of key points:*

* *We will be sending out these emails once a month, on a random day and time. Each month will be different.*
* *If you fall victim to one of these phishing emails the phishing simulation software will automatically notify you. However, your name is not reported to management or anyone on the security team, it will not impact you in anyway. This training is designed to help you learn. We are all in this together.*
* *Twenty-four hours after each assessment we will send an email out to everyone explaining the phishing simulation and how you could have identified the email was a scam or attack.*

*If you have any questions about this program or suggestions on how to improve it, please contact [Your Contact Information Here]. She is overall responsible for our security awareness program and will be happy to hear from you.*

# Phishing Assessment Follow-up

Example of an email used to follow-up after a phishing simulation.

*Folks,*

*As some of you may have noticed we had our monthly phishing simulation this week.  As always the purpose of these simulations is to help you identify and protect yourself against common email based attacks.  I've attached at the bottom of this email a screenshot of the simulation that went out.  If this had been a real attack, simply clicking on the URL in the email could have infected your computer.  There were some very simple ways to determine that this was a scam.*

*1. The email was extremely generic in nature.  Notice how it does not have your name but uses the introduction "Dear Customer" instead. The attack is designed to work against anyone.  If your bank had sent you an email it would have used your name.*

*2. Notice how the email creates a strong sense of urgency, trying to rush you into making a mistake.*

*3. Notice how the email comes from a @hotmail.com account, your bank would never use such an email address.*

*As for the simulation, only 8% fell victim. Great job folks. Finally, be sure to download this month's security awareness newsletter "Social Engineering" from our internal company portal.  As always, if you have any questions (or suggestions) about security, please contact the help desk.*

*Thanks!*

**NOTE**: Be sure to include screenshot of the attack in the email so people can read and learn from it.

# Responding to Reported Phishing Emails

If you are training your workforce to report phishing attacks, you need to ensure you always respond to any reported email. Positive feedback like this ensures people will continue to report. If someone reports a suspected attack and receives no response, they are far less likely to report again. Keep in mind, when someone reports a phishing email they have no idea if the phish was part of your phishing simulation or a real attack. Do not clarify either way, simply recognize them for their efforts and the impact it has.

*Dear [Name],*

*Thank you so much for your phishing submission, our security team greatly appreciates it. Our team will review the email and quickly act accordingly. We work extremely hard at and invest a tremendous number of resources in ensuring phishing attacks do not get through our networks, unfortunately we cannot identify or stop them all, especially customized targeted attacks. It’s because of people like you we are far more secure. Keep up the amazing work, we greatly appreciate it!*

*Your dedicated (and appreciative) information security team.*