# SECURITY AWARENESS

## DEPLOYMENT GUIDE SECURELY WORKING AT HOME

BULLETPROOF • IT
saving time • saving money • saving you

# Executive Summary

*As a result of Coronavirus, many organizations are finding themselves transitioning their workforce to work from home.*

This can be a challenge as many organizations lack the policies, technology and training to secure a remote workforce. In addition, many employees may be unfamiliar or uncomfortable with the idea of working from home.

**The purpose of this guide is to enable you to quickly train those people to be secure as possible.** If you have any questions on how to use this guide, reach out to us at or call us at 1.800.842.9452 or email us at info@bulletproofIT.ca.

Since your workforce is most likely going through a great deal of both stress and change, and your organization is most likely limited by time and resources, this strategic guide focuses on making the training as simple as possible.

We recommend you focus just on the most important risks that will have the greatest impact, which we describe below. **Think of these as a starting point.** If there are additional risks or topics you want to add, by all means, do. Just realize the more behaviors, processes or technologies you require of your workforce, the less likely they can implement all of them.

BULLETPROOF•IT
saving time • saving money • saving you

# How to Use This Guide

*We recommend you begin by reading the material in this guide and review the links to the different materials provide to give you an idea of what is available. You will notice that for each risk we provide a variety of different materials that you can use to engage and train your organization.*

**This enables you to select the modalities you feel will most effectively work for your needs and culture. Once you have reviewed the documentation there are two key groups you need to coordinate with.**

1

### 1. Security Team

Coordinate with your security team to gain a better understanding of what key risks you are attempting to manage. We have identified in this guide what we feel are the top, most common risks for a workforce working at home but your risks may be different. A word of caution, a common mistake security teams make is attempting to manage all risks and overwhelm people with numerous policies and requirements. Try to limit the risks you will address to as few as possible. Once you have identified and prioritized those risks, confirm the behaviors that will manage those risks. As already mentioned, if your organization does not have the time or resources for this, then leverage what we document below.

### 2. Communications

Once you have identified your top human risks and the key behaviors to manage those risks, then partner with your communications team to engage and train your workforce on those behaviors. The most effective security awareness programs have strong partnerships with their communications team. If possible, see if you can even embed someone from communications into your security team. When communicating to your workforce, an effective hook you can use to engage them is emphasize that not only will this training secure them at work but enable them to create a Cybersecure home, protecting themselves and their family.

2

*Ultimately by working with these two groups you are attempting to make security both as simple as possible for your workforce and motivate your workforce, the two key elements to behavior change.*

*We suggest you even create an Advisory Board of key people whose feedback and input you need to roll out the program. Besides your security and communications team, other departments you may want to partner and coordinate with include Human Resources and Legal.*

BULLETPROOF·IT
saving time • saving money • saving you

## Responding to Workforce – Questions and Incident Reporting

In addition to communicating to and training your workforce, we highly recommend some type of technology or forum where you can answer peoples' questions and/or report incidents, preferably in real-time. This can include a dedicated email alias, Skype or Slack chat channel, or some type of online forum such as with Yammer. The goal is you want to make security as approachable as possible and help people with their questions. In addition, having such an interactive platform with your workforce enables you to quickly identify and respond to incidents. This is a fantastic opportunity to engage your workforce and put a friendly face on security, try to take advantage of this.

*Keep in mind, for this to be effective we recommend dedicate a resource to moderate any security channels and actively respond to queries or reported incidents.*

## MGT433 Digital Download Package

SANS Institute provides the two-day training course MGT433: How to Build, Maintain and Measure a High-Impact Security Awareness Program. This intense class provides all the theory, skills, framework and resources to build a high impact awareness program enabling you to effectively manage and measure your human risk. As part of this guide we are providing free access to the course's Digital Download Package of templates and planning resources. While most likely above and beyond the needs of this initiative, these materials may be valuable for larger organizations or more complex deployments.

## Risks & Training Materials

We have identified three core risks you should manage for your remote workforce. These are a starting point and most likely the ones that will have the greatest value for you. Each risk below has links to multiple resources to help communicate and train the topic.

We provide multiple communication materials so you can select the ones that will have the greatest impact for your culture. In addition, almost all the materials come in multiple languages.

*If all of this is overwhelming and your time is extremely limited, then we recommend you simply go with and deploy the two materials listed below.*

1. Securely Working from Home Factsheet.

2. Creating a Cybersecure Home video (English)
also available in other languages here

## Social Engineering

One of the greatest risks remote workers will face, especially in this time of both dramatic change and an environment of urgency, is social engineering attacks. Social Engineering is a psychological attack where attackers trick or fool their victims into making a mistake, which will be made easier during a time of change and confusion.

**The key is training people what social engineering is, how to spot the most common indicators of a social engineering attack, and what to do when they spot one.** Be sure you do not focus on just email phishing attacks, but other methods to include phone calls, texting, social media or fake news. You can find the materials you need to train and reinforce this topic in our Social Engineering Support Materials folder. In addition, here are two SANS Security Awareness videos you can link to, once again provided in multiple languages.

**Social Engineering (English)**
*also available in other languages here*

**Phishing (English)**
*also available in other languages here*

### Strong Passwords

*As identified in the annual Verizon DBIR, weak passwords continue to be one of the primary drivers for breaches on a global scale. There are four key behaviors to help manage this risk, listed below. You can find the materials you need to train and reinforce this topic and these four key behaviors in our Passwords folder.*

**Passphrases** *(note, both password complexity and password expiration is dead)*

**Unique passwords for all accounts**

**Password Managers**

**MFA** (Multi-Factor Authentication).
*Often called Two-factor Authentication or Two-Step Verification*

## Updated Systems

The third risk is ensuring any technology your workforce uses is running the latest version of the operating system, applications and mobile apps.

For people using personal devices this may require enabling automatic updating. You can find the materials you need to train and reinforce this topic in the Malware or Creating a Cybersecure Home folders.

## Additional topics to consider

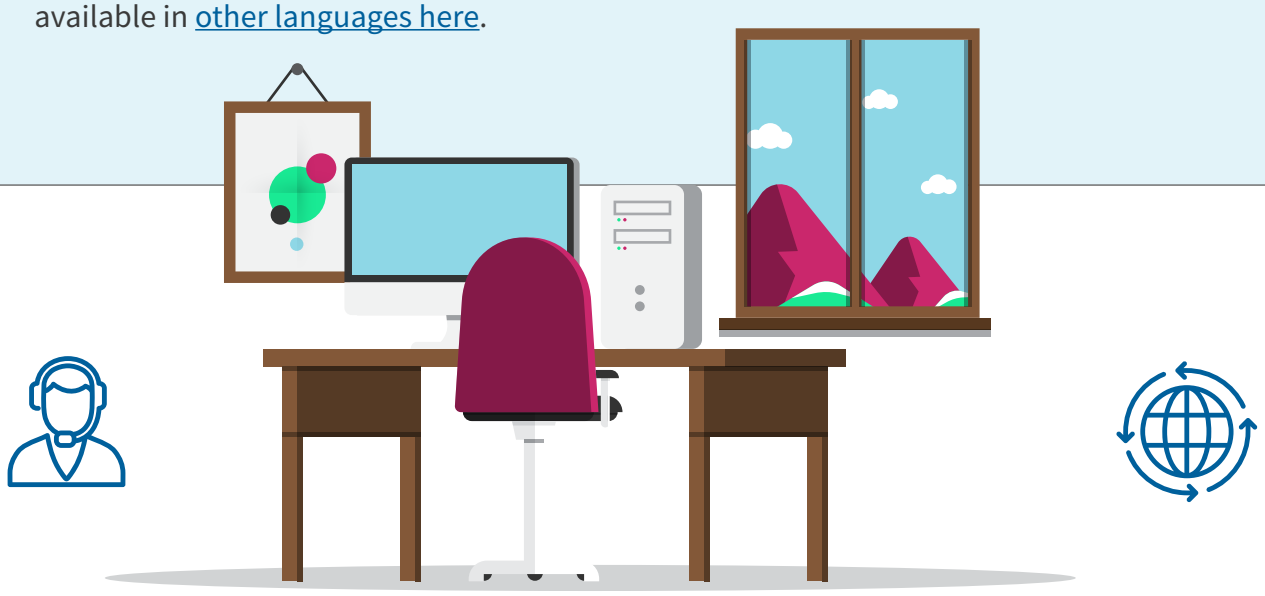
**Detection / Response:** Do you want people reporting if they believe there has been an incident while working at home? If so, what do you want them to report and when? This is covered our Hacked materials. For this to truly be effective ensure you have an easy channel for people to report suspicious activity. This will be especially critical when you have people working remotely.

**Wi-Fi:Securing your Wi-Fi access point:** This is covered in the Creating a Cybersecure Home materials Also, please consider this video on Creating a Cybersecure Home Video (English) also available in other languages here.

**VPNs:** What is a VPN and why you should use one. We recommend the OUCH newsletter on VPNs.

**WorkingRemotely:** This is for individuals who are working remotely but NOT working from home, such as a coffee shop, airport terminal or hotel. Consider using our Working Remotely training video (English) also available in other languages here.

**Children / Guests:** To reinforce the idea that family / guests should not access work related devices, consider using the Working Remotely training video (English) also available in other languages here.



# OVERVIEW

### FOUR STEPS TO STAYING SECURE
https://www.sans.org/security-awareness-training/resources/four-simple-steps-stayingsecure

### CREATING A CYBERSECURE HOME
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creatingcybersecure-home

### SOCIAL ENGINEERING
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

### MESSAGING / SMISHING
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

### PERSONALIZED SCAMS
https://www.sans.org/security-awareness-training/resources/personalized-scams

### CEO FRAUD
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

### PHONE CALL ATTACKS / SCAMS
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

### STOP THAT PHISH
https://www.sans.org/security-awareness-training/resources/stop-phish

### SCAMMING YOU THROUGH SOCIAL MEDIA
https://www.sans.org/security-awareness-training/resources/camming-you-throughsocial-media

BULLETPROOF•IT
saving time • saving money • saving you