SANS SECURITY AWARENESS

Security Awareness Deployment Guide – Securely Working at Home

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 support@sans.org.

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.

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. **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.

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.

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. Keep in mind, for this to be effective we recommend dedicating a resource to moderate any security channels and actively respond to queries or reported incidents. In addition, ensure you have strong authentication mechanisms allowing only authenticated users to these platforms. As your Help Desk / Security teams are overwhelmed with questions, this is also prime time for cyber attackers to attempt to socially engineering them, such as for password resets, VPN configurations, etc.

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 (included in your Deployment Kit).
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 in 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.

- **Working Remotely**: 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.

OUCH Newsletters

In addition, consider using the publicly available OUCH newsletters to support your program, each translated into over twenty languages. Listed below are the OUCH newsletters that we feel can best support your Securely Working at Home initiative. You can find all newsletter at the online OUCH Security Awareness Newsletter Archives.

OVERVIEW

Four Steps to Staying Secure
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

SOCIAL ENGINEERING

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/scamming-you-through-social-media

PASSWORDS

Making Passwords Simple
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

ADDITIONAL

Yes, You Are a Target
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Quick Tips

Tips and tricks you can share in easily to consume format.

- The most effective steps you can take to secure your wireless network at home is to change the default admin password, enable WPA2 encryption and use a strong password for your wireless network.
- Be aware of all the devices connected to your home network, including baby monitors, gaming consoles, TVs, appliances or even your car. Ensure all those devices are protected by a strong password and/or are running the latest version of their operating system.
- One of the most effective ways you can protect your computer at home is to make sure both the operating system and your applications are patched and updated. Enable automatic updating whenever possible.
- Ultimately, common sense is your best protection. If an email, phone call or online message seems odd, suspicious or too good to be true, it may be an attack.
- Make sure each of your accounts has a separate, unique password. Can't remember all of your passwords/passphrases? Consider using a password manager to securely store all of them for you.
- Two-step verification is one of the best steps you can take to secure any account. Two-step verification is when you require both a password and code sent to or generated by your mobile device. Examples of services that support two-step

verification include Gmail, Dropbox and Twitter.

- Phishing is when an attacker attempts to fool you into clicking on a malicious link or opening an attachment in an email. Be suspicious of any email or online message that creates a sense of urgency, has bad spelling or addresses you as "Dear Customer."

Metrics

Behavioral metrics are difficult for this situation as it is more difficult to measure how people behave at home. In addition, some of these behaviors are not work specific (such as securing their Wi-Fi device). However, you can measure engagement. We have found that personal or emotional topics like these can be very engaging, drawing far greater interest than other topics. As such, metrics like these may be of value.

- **Interaction**: How often are people asking questions, posting ideas or requesting help on any of the security channels or forums you are hosting?
- **Simulations**: Conduct some type of social engineering simulations, such as phishing, texting or phone call-based attacks.

For a far more comprehensive list of metrics, download the interactive Security Awareness Metrics Matrix from the MGT433 Digital Download Package.

Appendix: Communications Template

The purpose of this template is to help you communicate and introduce the concept of working from home. We highly recommend that you coordinate this message with / through your communications department as your organization is most likely already actively communicating about the Coronavirus. Below is an example of what you can communicate - however be sure to modify this to your needs and requirements.

Folks, as you prepare to work from home, one of our goals is to help you do safely and securely. As such, over the next couple of days / weeks we will be sharing with you key steps and tips on how you can work securely from home. At times Cybersecurity may seem overwhelming, however by following just some simple, basic steps you will go a long way to protecting yourself. In addition, everything you will be learning not only applies to work but will help protect your family and personal life, ultimately creating a far more Cybersecure home for. The key topics we will be focusing on to help secure you are

- ***Social Engineering**: How to spot and stop social engineering attacks, such as those that happen over the email or the phone.*
- ***Home Network**: Key steps to securing your home network, stating with your Wi-Fi device.*
- ***Passwords**: How to use passwords safely and securely.*
- ***Updating**: How to make sure you are always using the latest and most current systems, applications and mobile apps.*
- ***Family / Guests**: How to handle family and guest for work-related devices and activities.*

Following just a few steps will go a tremendous way to securing you and your family at home. If you have any questions about working securely at home or suggestions on how to improve our cyber security efforts, please contact [Your Contact Information Here]. She is overall responsible for our security awareness program and will be happy to hear from you.

[**NOTE**: You can put your security team's contact information at the end or perhaps link to your internal security portal, security channels or any other resources you may want to promote].

License

Deployment Kit Author

Lance Spitzner has over 20 years of security experience in cyber threat research, security architecture and awareness and training. He helped pioneer the fields of deception and cyber intelligence with his creation of honeynets and founding of the Honeynet Project. As a SANS instructor he developed the MGT433:Security Awareness and MGT521: Security Culture courses. In addition, Lance has published three security books, consulted in over 25 countries and helped over 350 organizations build security awareness and culture programs to manage their human risk. Lance is a frequent presenter, serial tweeter (@lspitzner) and works on numerous community security projects. Before information security, Mr. Spitzner served as an armor officer in the Army's Rapid Deployment Force and earned his MBA from the University of Illinois

About SANS Institute

The SANS Institute was established in 1989 as a cooperative research and education organization. SANS is the most trusted and, by far, the largest provider of cyber security training and certification to professionals at governments and commercial institutions world-wide. Renowned SANS instructors teach over 60 different courses at more than 200 live cyber security training events as well as online. GIAC, an affiliate of the SANS Institute, validates a practitioner's qualifications via over 35 hands-on, technical certifications in cyber security. The SANS Technology Institute, a regionally accredited independent subsidiary, offers master's degrees in cyber security. SANS offers a myriad of free resources to the InfoSec community including consensus projects, research reports, and newsletters; it also operates the Internet's early warning system--the Internet Storm Center. At the heart of SANS are the many security practitioners, representing varied global organizations from corporations to universities, working together to help the entire information security community. (https://www.sans.org)