SANS SECURITY AWARENESS

Security Awareness Deployment Guide – Working From Home

Deployment Plan

Organizations need to enable their workforce to work securely and safely at home as a result of the Coronavirus. This is a challenging transition as this is something many employees may be unfamiliar or uncomfortable with. The purpose of this Deployment Guide is to enable your security team to quickly train those people to be secure as much as possible. Since your workforce is most likely going through a great deal of change, and you are limited by time, we recommend your focus on a select few of the most important behaviors that will have the greatest impact.

Below are the risks we suggest you focus on. 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, policies, processes or technologies you require of your workforce, the less likely they can implement all of them.   To learn more about prioritizing and managing human risk, consider the SANS MGT433 course which is offered online.

In addition to communicating the topics below, we highly recommend some type of technology or forum where you can answer peoples' questions, 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. Another idea is hosting a security webcast that you repeat several times a week so people can pick a time that works best for them and attend the event live, perhaps even ask questions. The goal is you want to make security as approachable as possible and help people with their questions. This is a fantastic opportunity to engage your workforce and put a friendly face on security, try to take advantage of this. However, this will require you to dedicate a resource to moderate these channels and / or respond to queries.

Risks & Training Materials

These topics are suggested as a starting point and most likely the ones that will have the greatest return on investment. Each topic below has links to resources to help communicate and train the topic.

- **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. These attacks can take on many forms, not just email based phishing attacks but phone calls, text messaging or over social media. The key is training people what social engineering is, the most common indicators of a social engineering attack, and what to do when they spot one. You can find the materials you need to train and reinforce this topic in our Social Engineering folder.

- **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. A key finding is strong passwords are one of the most effective defenses. You most likely want to re-emphasize the need for strong password use by focusing on these four key behaviors. You can find the materials you need to train and reinforce this topic and these four key behaviors in our Passwords folder.

  - Passphrases (password complexity 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 topic is ensuring any technology your workforce uses are using is running the latest version of the operating system, applications and mobile. For personnel 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 folder.

Additional topics you can consider include

- **Wi-Fi**: How to secure a Wi-Fi access point. This is covered in the Creating a Cybersecure Home materials.

- **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 any of our Hacked materials.

Publicly Available Resources

In addition, here are freely available resources that can help reinforce these three specific risks. For other topics check out the 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

Virtual Private Networks
https://www.sans.org/security-awareness-training/resources/virtual-private-networks-vpns

Quick Tips

Daily tips specific to this month’s topic.

- 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.