1. Main Page Description

October is internationally recognized as Cybersecurity Awareness Month. Started in 2004 as a partnership between the US Department of Homeland Security and the non-profit National Cyber Security Alliance, this month is now globally recognized. In the United States it was originally called National Cyber Security Awareness Month (NCSAM) but is now known as Cybersecurity Awareness Month (CAM). In Europe it is known as European Cybersecurity Month (ECSM) and run by ENISA. The goal of this global event is to create awareness about cybersecurity and to enable people to secure themselves and their organizations. To help you and your organization make the most of this October, SANS Security Awareness has created the CAM Planning Toolkit. This kit contains resources such as presentations, newsletters, tips and other materials. This kit is designed to work on its own or supplement anything you may already have planned. If you have any questions or suggestions on this community resource, please contact us at sth-community@sans.org.

2. Themes

The theme for CAM 2020 is “Do Your Part, #BeCyberSmart” with the #BeCyberSmart the primary hashtag used in social media. As per the NCSA website

The theme empowers individuals and organizations to own their role in protecting their part of cyberspace, with a particular emphasis on the key message for 2020: If you connect it, protect it.

The NCSA has created weekly themes for the month of October. You are in no way required to follow these themes and encouraged to create your own themes that are most relevant to your organization.

- Week 1 / 2 October: Official kick-off for the month
- Week of 5 October (Week 1): If you Connect It, Protect It
- Week of 12 October (Week 2): Securing Devices at Home and Work
- Week of 19 October (Week 3): Securing Internet-Connected Devices in Healthcare
- Week of 26 October (Week 4): The Future of Connected Devices
3. Make the Most of CAM

Often the temptation for this month is to create as much noise and throw out as many flashy materials and events as possible. Instead, we recommend focus on just the most important risks that will have the greatest impact. Not sure what your greatest human risks are? Below we have identified what we feel are the top, most common risks for today’s workforce working at home. 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 you will be able to remember and exhibit those behaviors. Not sure what your top risks are? Coordinate with your security team to gain a better understanding of what key risks you are attempting to manage. As already mentioned, if your organization does not have the time or resources for this, then leverage what we document below.

4. Top Risks / Topics

Risk #1: 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 site. 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

Risk #2: 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

**Risk #3: 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.

• **Virtual Conferencing**: Top tips for both attending a virtual conference or hosting a virtual conference.
5. 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**
Online Security for Kids
https://www.sans.org/security-awareness-training/resources/online-security-kids

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/resources/creating-cyber-secure-home

**SOCIAL ENGINEERING**
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
Appendix A: Communications Template

Start any Cybersecurity Awareness Month (CAM), often called European Cybersecurity Month (ECSM) in Europe, by communicating to people why they should care about cybersecurity and this month. You need to create excitement and buzz about cyber security. One approach is focusing on how people will personally benefit. By focusing on peoples’ personal lives, they are far more likely to be engaged. In addition, the same secure behaviors apply to both home and work, so your organization benefits also. If possible, have the most senior executive from your organization announce the upcoming events, such as the CFO or CEO. Here is one possible email you could use, edit as you see fit. Keep in mind you are not limited to just email for your communications, other options include having an executive announce CAM through a blog, corporate video, internal social media such as Yammer or some other means. The more creative you are the greater the impact.

Folks, we know that you have a lot of questions about cyber security, especially about what you can do at home to protect yourself and your family. That is why we are so excited to announce a series of activities next month during Cybersecurity Awareness Month. During October, you will have the chance to participate in a variety of events and collect numerous resources to help you better understand cyber security and the simple steps you can take to protect yourself, your family and our organization. Our goal is to enable you to make the most of today’s technology. And in case you were wondering, yes, I will be participating in these many activities next month. Please take them seriously and apply what you learn. I look forward to seeing the results and hearing your feedback.

If you have any questions about our activities in October 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 or self-education site].