California Community Colleges | Information Security Center

Remote-Work Security Practices:
A Guide for California Community Colleges | March 2020

Prepared by Aamir Khan, Interim Chief Information Security Officer, and Omer Usmani, Security Analyst, California Community Colleges Information Security Center

The purpose of this guide is to introduce common security practices when working remotely. Before distributing this information with your district or college, it is recommended that you coordinate this message with the relevant department. Your district may have already communicated about working from home.

Overview

Below is an outline of recommended practices remote workers can take to enhance their cyber security measures in order to prevent a breach of important information. This guide has gathered and presented resources from SANS, ISAC, CIS, and the California Community Colleges (CCC) Technology Center. The primary topics of discussion include the following:

1. **Social Engineering:** How to identify and prevent social engineering attacks, which are primarily executed through phone or email.

2. **Home Network Security:** Important steps to secure a home network, beginning with Wi-Fi devices.

3. **Passwords:** How to utilize and manage secure passwords.

4. **Software Updates:** Ensuring the latest security patches have been applied to all operating systems, mobile applications, and devices.

We recommend you first begin by reading this guide and then review the links to the various sources of material provided to give you an idea of what is available. The training videos and articles presented in this document and appendices are published by SANS, ISAC, CIS, and the CCC Technology Center. You will see that for each respective risk, there are a multitude of materials that can be utilized to train employees. It is recommended that you select material

that you feel will most effectively work for your district or college. We do not intend to overwhelm workers with numerous sources of information presented at once.

Once you have reviewed all the material, there are two teams you should coordinate with:

1. **Information Security:** Work with your information security team to obtain an idea of the key risks your district or college is attempting to manage. This guide contains the common risks to look at when working from home, but risks for specific groups of employees may be different. As mentioned above, we do not want you to overwhelm your staff. Try to limit the risks you want to address and prioritize what you feel is most important. Once you have identified priority risks, implement practices that will manage those risks. If your district or college does not have the resources or time to do this, please utilize the information in this guide as effectively as you can.

2. **Communications**: Work with your communications team to relay information to staff members about the risks you have identified and the practices they can take to minimize them.

By coordinating with these two groups, you are attempting to make the process of implementing security measures easier on your staff. Other departments you may consider partnering and coordinating with include Legal and Human Resources.

Key Risks and Appropriate Training Material

There are three general threats for which you should consider remote workers at risk. For each of the risks outlined below, we include links to a relevant SANS training video, or documentation that summarizes the risk and prevention measures.

1. Social Engineering

The first major risk to consider is social engineering attacks. This is where an attacker(s) attempts to take advantage of an unsuspecting user in order to obtain confidential information or the means to access that information. This process is simplified when staff members transition out of the office into their own homes.

The materials linked below will help users identify common aspects of social engineering, and the steps they need to take if they suspect they have been targeted. These materials cover email phishing attacks as well as phone calls, text messages, and social media. See Appendix A for additional resources related to social engineering attacks.

SANS Social Engineering Video
SANS Phishing Video
ES-ISAC Article – Social Engineering

2. Home Network Security

The second major risk is having an unsecured home network. Wireless networks are the general means of connectivity in homes, usually controlled by a router setup by an ISP. The first thing a remote worker would want to change is the default administrator password to access the router's configuration dashboard. This should comply with password complexity guidelines, covered in the next section. They should also make sure that the password is WPA2 encrypted, which can be configured in the router's dashboard. A remote worker should also consider setting up a separate guest network. This is done through the router's configuration settings as well. Having a separate network for guests will prevent them from potentially accessing work devices. Additional tips are provided in the video below:

SANS Creating a Cybersecure Home Video (English)

3. Passwords

The third major risk is weak passwords. According to the latest Verizon Data Breach Investigations Report, weak passwords are the primary vulnerabilities that result in data breaches. Following are four general recommendations your district or college can take to help mitigate this risk:

- Use password managers (e.g.,. LastPass, 1Password, Google Password Manager)
- Have your organization implement two-factor authentication (e.g., Duo)
- Do not share credentials with anyone
- Implement a cycle in which passwords are required to be reset

More information regarding password recommendations is provided in the MS-ISAC article, linked below.

MS-ISAC Security Primer – Securing Login Credentials

4. Software Updates

The fourth major risk is outdated software, which is often open to vulnerabilities. Try to provide the latest version of an operating system, applications, and other devices you may distribute to employees. This may require enabling automatic updates. Here are materials you can relay to remote workers:

SANS "You Are a Target" Article
SANS Malware Material

Additional Topics to Consider

VPNs: What is a VPN, and why should you use one when working from home? Please take a look at these recommendations from Consumer Reports.

Detection / Response: To give your remote workers a general idea of what to do if they are involved in or suspect being involved in an incident, take a look at the SANS training "Hacked" material.

Family & Guests: To reinforce the idea that family or visiting guests should not use devices related to your workplace, watch the SANS Working Remotely Training Video.

Working Remotely: This is for individuals who are working remotely outside of their own home (i.e. coffee shop, hotel, or airport terminal). Please refer again to the SANS Working Remotely Training Video.

Information Security Mailing List

In addition to reviewing the tips above, consider having your employees subscribe to our information security mail list. We provide updates regarding common vulnerabilities, exploits, and patches for commonly used products.

https://cccsecuritycenter.org/services/is-mailing-list

For more information on the contents of this guide, please contact:

Omer Usmani
Security Analyst
Information Security Center
California Community Colleges Technology Center
ousmani@ccctechcenter.org

APPENDIX A: Information Security Tips and Training Videos

In addition to the resources provided in the Remote-Work Security Practices guide, we have compiled a list of relevant SANS training videos you can distribute to remote workers.

General Tips

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

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

Social Engineering

Social Engineering
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing Attacks
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 B: Cyber Hygiene Best Practices

This is an addendum to the tips discussed in the Remote-Work Security Practices guide.

Overview

Cyber Hygiene: Conceptualizing cybersecurity practice in terms of personal hygiene practices.

- Germ Theory: An accepted scientific theory for many diseases. Microorganisms and pathogens can lead to disease, but cannot be viewed with the naked eye.

- Similarly, people rarely see the exploits or socially engineered cyberattacks until it is too late.

- We accept that germs can make us sick, and we're willing to take precautions to practice good hygiene on a daily basis to guard against them (ie. washing hands, taking showers, taking medications).

- In a similar fashion, to keep digital viruses away, you need to implement hygienic practices to protect both you and your organization.

Common Ways Data is Compromised:

- Password Theft
- Phishing
- Ransomware

Password Theft

1. **How passwords work**

   Common ways passwords are breached are through GPU-based cracking tools and social engineering, including phishing.

   a. Password complexity is the best way to prevent password theft.
      i. Example: Michael Linton, former Sony CEO used "sonyml3" as his password. Passwords for internal accounts were stored under a file called "passwords".
   b. Passwords are not saved as plain text, e.g., "abcd1234"
      i. They are encrypted by a hash algorithm, e.g., "abcd1234" under MD5: "e19d5cd5af0378da05f63f891c7467af"

2. **How passwords are cracked**

   a. Hashes are obtained through exploiting a known vulnerability on a system (e.g. SQL Injection) and extracting the user database containing password hashes.
   b. Systems that have LLMNR or NBT-NS enabled can be compromised through tools such as Responder.

i. Responder is an open source tool used to poison named services to gather hashes and credentials from systems within a local network.

c. Once hashes are obtained, a password cracking tool is used to check a pre-compiled list of passwords against the available hashes of an account.
   i. DICTIONARY/WORDLIST ATTACK = Uses a precompiled list of words, phrases, and common/unique strings to attempt to match a password.
   ii. BRUTE-FORCE ATTACK = attempts every possible combination of a given character set, usually up to a certain length.
   iii. RULE ATTACK = generates permutations against a given wordlist by modifying, trimming, extending, expanding, combining, or skipping words.
   iv. Example: John the Ripper, Hashcat

d. Ordinary desktop computers can test over a hundred million passwords per second using password cracking tools running on a general purpose CPU

e. Billions of passwords per second using GPU-based password cracking tools
   i. CPU = 2-72 cores mainly optimized for sequential serial processing
   ii. GPU = 1000's of cores with 1000's of threads for parallel processing

f. A longer password makes it difficult to crack, even for a supercomputer

Reasonably efficient:

	phpass	sha256crypt	sha512crypt	md5crypt	bcrypt	MSCash2	WPA-PSK	RAR	Password Safe
CUDA	Yes	Yes	Yes	Yes		Yes	Yes		Yes
OpenCL	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Password Length	Possible Combinations	Time To Crack (s = Seconds, m = Minutes, h = Hours, y = Years)
4	45697	<1 s
5	11881376	<1 s
6	308915776	<1 s
7	8031810176	~4 s
8	208827064576	~1.5 m
9	5429503678976	~45 m
10	141167709565337 6	~19 h
11	3670344486987780	~.1 y
*12	95428956661682200	~1.5 y
13	248115287320374E4	~39.3 y
14	6450997470329 72E5	~1,022.8 y
15	1677259342285 73E7	~26,592.8 y
16	4360874289942 89E8	~691,412.1 y
17	1133827315385 15E10	~17,976,714 y
18	2947951020001 390E10	~467,394,568 y

3. What can you do?

a. Use a password manager such as LastPass, 1Password, iCloud Keychain, or Google Password Manager.

b. Have your organization implement two-factor authentication (e.g., Duo).

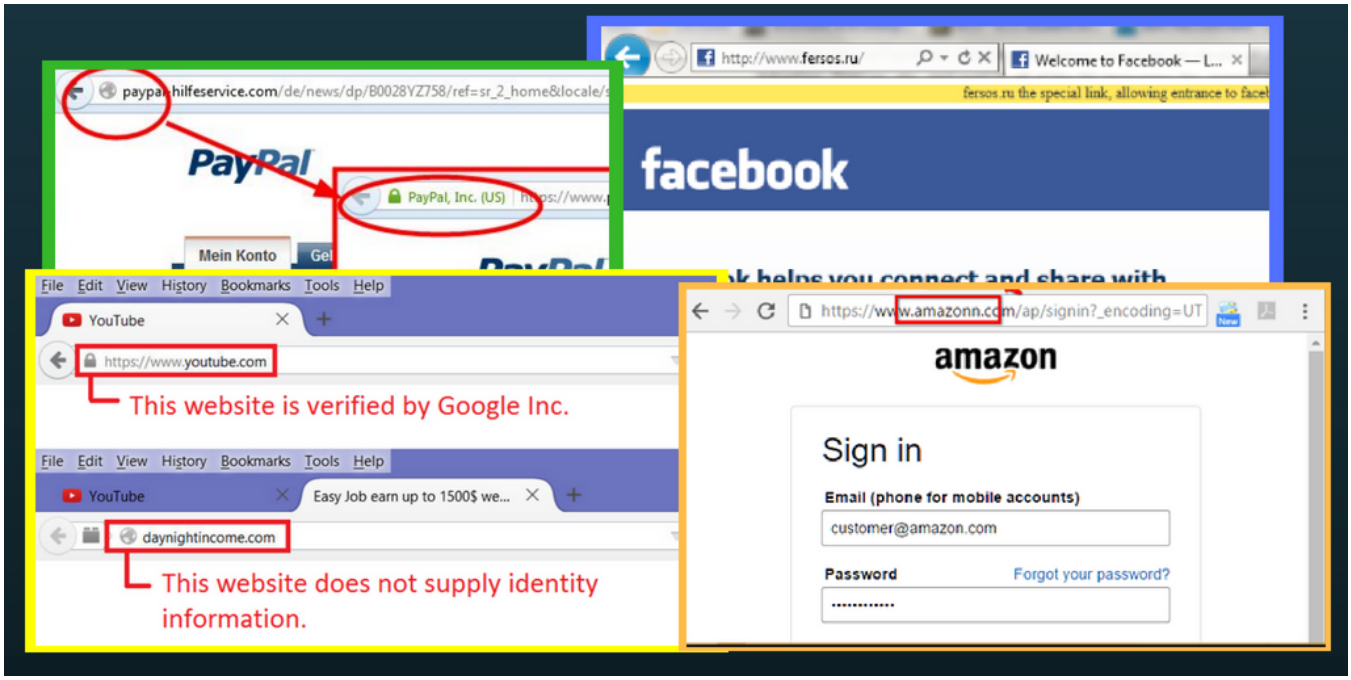
c. Do not share credentials with anyone.

d. Have a cycle where passwords are required to be reset.

e. System administrators should disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment.

Phishing

1. **Email & Browsing Hygiene**
   a. Always keep in mind, “Does the direct email relate to a matter that I am involved in?”
   b. Do not enter information in websites without “https” in beginning of address (lock symbol)
      i. Communication is encrypted. Personal information entered cannot be immediately viewed.
      ii. According to the World Website Consortium, 59 percent of websites use an https protocol.
      iii. Google: 71 of the world’s top 100 websites use https.
   c. Be wary of emails that imply urgency regarding passwords or account information:
      i. “Change password immediately”
      ii. “Your mailbox is out of space”
      iii. “There was a problem with your credit card information”
      iv. ”We have migrated to a new ……: Click Here”.
2. **Look out for URL manipulation**
   a. Common for attackers to provide a link with a slight modification to the URL or subdomain of the intended website.
      i. http://www.bankofamerica.example.com/
   b. Another trick is to edit the content of an HTML tag to make it look like it goes to a legitimate website. The link actually goes to a malicious website.
      i. <h6><a href=www.maliciouswebsite.com>www.bankofamerica.com</h6>



Examples of modified addresses

Ransomware

Ransomware is a form of malware designed to encrypt a target system's files. It Involves a payment to regain access, commonly in BitCoin. This can be orchestrated through phishing attempts. In this case a malicious file would be downloaded onto the victim's system causing files to be encrypted. The malware can spread to other devices on the same network.

1. **Process**
   a. [attacker → victim] The attacker generates a key pair and places the corresponding public key in the malware. The malware is released.
   b. [victim → attacker] Malware generates a random symmetric key that encrypts the victim's data. It uses the public key in the malware to encrypt the symmetric key. Message is displayed to the user that includes asymmetric ciphertext and how to pay the ransom. The victim sends the asymmetric ciphertext and e-money to the attacker.
   c. [attacker → victim] The attacker receives the payment, deciphers the asymmetric ciphertext with the attacker's private key, and sends the symmetric key to the victim. The victim deciphers the encrypted data with the needed symmetric key.

   Proceedings 1996 IEEE Symposium on Security (PDF) and Privacy

2. **Example & Prevention**
   a. NotPetya: A variant of encrypting ransomware Petya.
      i. In June 2017, attackers targeted businesses and government institutions in France, Germany, Italy, Poland, and the United Kingdom. They demanded $300 worth of bitcoin to decrypt the compromised devices.
      ii. This was only a decoy, because files were being deleted anyway.
      iii. Total loss was over $10 billion.

3. **Proper Hygiene**
   a. Keep up with operating system and software updates.
   b. A Windows Security update, MS17-010, released months before the NotPetya ransomware incident, could have prevented the attack.