California Community Colleges | Technology Center

Teleworking Security Guidelines

Prepared By
Aamir Khan
CCCTC CISO
&
Omer Usmani
CCCTC Security Analyst

Introduction

The intention of this guide is to help you get introduced to 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.

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 CCC Tech Center. The primary topics of discussion include the following:

- ***Social Engineering:*** How to identify and prevent social engineering attacks, primarily executed through phone or email.
- ***Home Network Security:*** Important steps needed to secure a home network, beginning with WI-FI devices.
- ***Passwords:*** How to utilize and manage secure passwords.
- ***Updating:*** Making sure operating systems, mobile applications, and devices are up to date and patched with the latest security fixes.

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 are published by SANS, ISAC, CIS, and the CCC Tech 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 to 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.

- ***Security Team:*** Work with your security team to obtain an idea of what key risks your district or school 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 on what you feel is most important. Once you have identified what you want to prioritize, implement practices that will manage those risks. If your district or college does not have the resources or time to do this, then please utilize the information in this guide as effectively as you can.

- ***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 process of implementing security measures easier on your staff. Other departments you may want to partner and coordinate with include Legal and Human Resources.

Key Risks and Appropriate Training Material

There are three general threats you should consider remote workers at risk for. Each risk outlined below has links to a relevant SANS training video, or documentation that summarizes the risk and efforts to prevent it. The video linked below regarding home network security can serve as a starting point for your staff.

SANS Creating a Cybersecure Home Video (English)

1) Social Engineering

The first major risk to consider are social engineering attacks. This is where an attacker(s) attempts take advantage of an unsuspecting user in order to hand over 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 provided below will help users identify common aspects of social engineering, and the steps they need to take if they suspect being targeted. These materials cover not only email phishing attacks, but also phone calls, text messages, and social media. Here are two SANS social engineering videos, as well as an EI-ISAC article on the topic.

SANS Social Engineering Video

SANS Phishing Video

ES-ISAC Article – Social Engineering

2) Weak Passwords

According to the latest Verizon DBIR (Data Breach Investigations Report), weak passwords are the primary culprit in the cause of data breaches. There are four general recommendations your district or college can take to help mitigate this risk, listed below. You can find more information regarding password recommendations in the MS-ISAC article linked below.

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

MS-ISAC Security Primer – Securing Login Credentials

3) Outdated Systems

The third risk is to mitigate is the use of 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 you should use one. 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). Refer to the SANS Working Remotely Training Video again.

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

OVERVIEW

We have provided a list of relevant SANS training videos you can distribute to remote workers, some of which were already linked above.

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 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

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

Cyber Hygiene: Overview & Tips

An addendum to the tips discussed above

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

- **Germ Theory →** Accepted scientific theory for many diseases. Microorganisms and pathogens can lead to disease, 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 company.

Common Ways Data is Compromised

1. *Password Theft*
2. *Phishing*
3. *Ransomware*

I. How passwords work

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

- Complexity is the best ways to prevent password theft.

    - Example: Michael Linton, former Sony CEO used "sonyml3" as his password. Passwords for internal accounts were stored under a file called "passwords".

- Passwords are not saved as plain text - "abcd1234"

- They are encrypted by a hash algorithm, "abcd1234" under MD5: – "e19d5cd5af0378da05f63f891c7467af"

How passwords are cracked

- Hashes are obtained through exploiting a known vulnerability on a system (e.g. SQL Injection) and extracting the user database containing password hashes

- Systems that have LLMNR or NBT-NS enabled can be compromised through tools such as Responder.

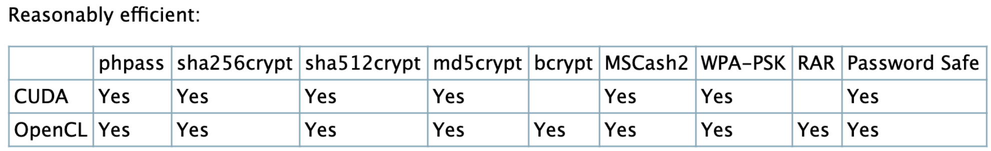
- Responder is an open source tool used to poison named services to gather hashes and credentials from systems within a local network.

- 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.
    - DICTIONARY/WORDLIST ATTACK = Uses a precompiled list of words, phrases, and common/unique strings to attempt to match a password.
    - BRUTE-FORCE ATTACK = attempts every possible combination of a given character set, usually up to a certain length.
    - RULE ATTACK = generates permutations against a given wordlist by modifying, trimming, extending, expanding, combining, or skipping words.

- E.g. John the Ripper, Hashcat

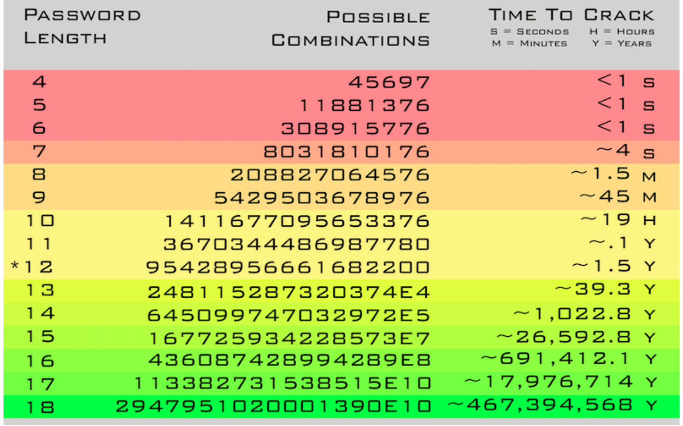
- Ordinary desktop computers can test over a hundred million passwords per second using password cracking tools running on a general purpose CPU

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



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 H = Hours
		M = Minutes 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	141167095653376	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	248115287320374E4	~39.3 Y
14	645099747032972E5	~1,022.8 Y
15	167725934228573E7	~26,592.8 Y
16	436087428994289E8	~691,412.1 Y
17	113382731538515E10	~17,976,714 Y
18	294795102000139OE10	~467,394,568 Y

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

What can you do?

- Use password managers: LastPass, 1Password, iCloud Keychain, Google Password Manager
- Have your organization implement two-factor authentication (e.g. Duo)
- Do not share credentials with anyone
- Have a cycle where passwords are required to be reset.
- System administrators should disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment.

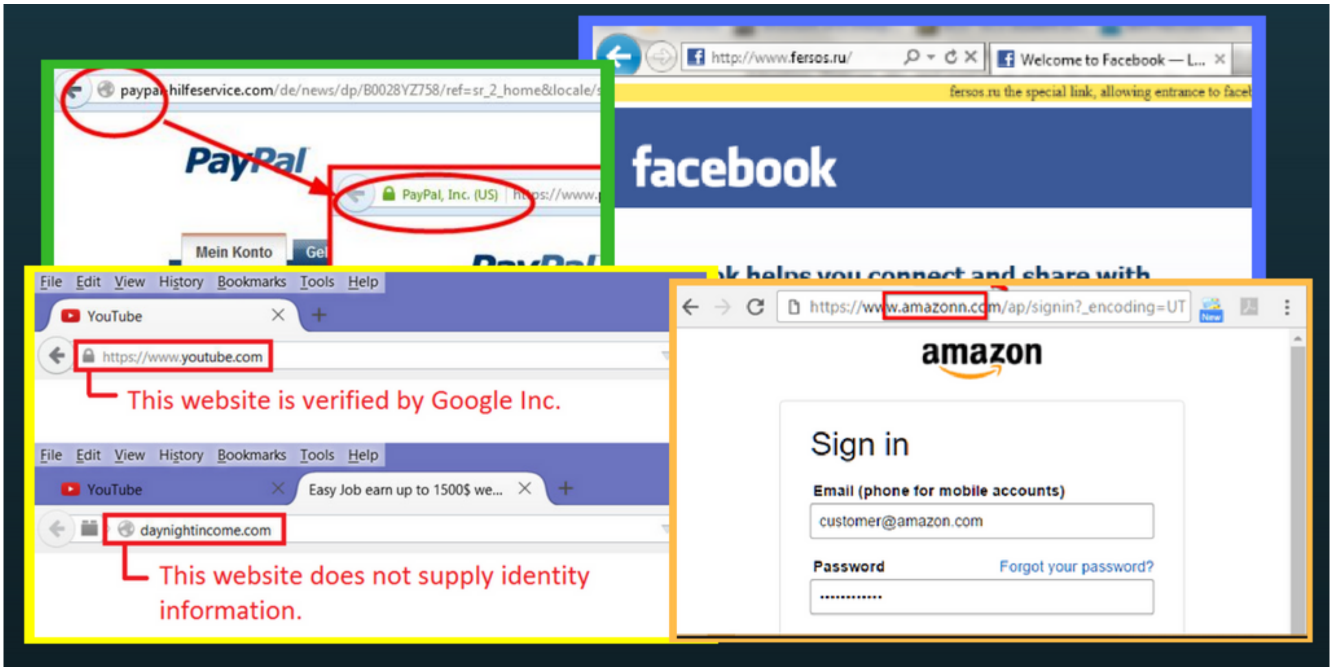
II. Phishing Protection

Email & Browsing Hygiene

1. Always keep in mind, "Does the directly email relate to a matter that I am involved in?"
2. Do not enter information in websites without "https" in beginning of address (lock symbol)
    - Communication is encrypted. Personal information entered cannot be immediately viewed.
    - According to the World Website Consortium, 59 percent of websites use an https protocol.
    - Google: 71 of the world's top 100 websites use https.
3. Be wary of emails that imply urgency regarding passwords or account information:
    - "Change password immediately"
    - "Your mailbox is out of space"
    - "There was a problem with your credit card information"
    - "We have migrated to a new ......: Click Here".

Look out for URL manipulation

- Common for attackers to provide a link with a slight modification to the URL or subdomain of intended website.
- http://www.bankofamerica.example.com/
- 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.
- <h6><a href=www.maliciouswebsite.com>www.bankofamerica.com</h6>


paypal hilfeservice.com/de/news/dp/B0028YZ758/ref=sr_2_home&locale/
PayPal
PayPal, Inc. (US) https://www.
Mein Konto
http://www.fersos.ru/
Welcome to Facebook — L...
fersos.ru the special link, allowing entrance to faceb
facebook
k helps you connect and share with
File Edit View History Bookmarks Tools Help
YouTube
https://www.youtube.com
File Edit View History Bookmarks Tools Help
YouTube
Easy Job earn up to 1500$ we...
daynightincome.com
https://www.amazonn.com/ap/signin?_encoding=UT
amazon
Sign in
Email (phone for mobile accounts)
customer@amazon.com
Password
Forgot your password?

This website is verified by Google Inc.

This website does not supply identity information.

Examples of modified addresses

III. Ransomware

- A form of malware designed to encrypt a target system's files.
- 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. Can spread to other devices on the same network.
- Files are encrypted

Process

1) [attacker→victim] The attacker generates a key pair and places the corresponding public key in the malware. The malware is released.
2) [victim→attacker] Malware generates a random symmetric key and encrypts the victim's data with it. 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.
3) [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 and Privacy

Example & Prevention

NotPetya

- Variant of encrypting ransomware Petya. 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 compromised device. This was only a decoy, because files were being deleted anyways. Total loss was over $10 billion.

Proper Hygiene: Keep up with operating system and software updates Windows Security update MS17-010 could have prevented this. Released in April 2017

Contact Information:

Questions or Comments may be directed to:

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