



Digital Security Training for Digital Citizens and Activists

October 26, 2021

This presentation has been delivered as part of
SomNOG5 Workshops and Conference via online



**WORKSHOPS AND CONFERENCE
23 - 28 October 2021**

**DIGITAL INFRASTRUCTURE
FOR DEVELOPMENT**



**@SomNOG
#DigitalSomalia**



**www.somnog.so
info@somnog.so**

Climate setting, introductions, participants' expectations & training objective

TOPIC TO BE COVERED

- **Digital Safety and Analyzing digital threats**
- **Digital data backups: Importance and tools**
- **Classification tips for misinformation and disinformation**
- **Introduction to digital encryption techniques (BitLocker and Tutanota)**
- **Virtual Private Network (VPN)**
- **Data recovery tools and techniques**
- **Dealing with social media trolls**

Participants Introductions:


Please share:

Your name, location, role, and how often you interact with data and internet both personally and professionally.

Introduction to Digital Security/Safety

Digital Security in COVID-19 era

CYBER SAFETY CHECKLIST




Back up online and offline files regularly and securely




Manage social media profiles




Strengthen your home network



Check privacy and security settings



Use strong passwords



Avoid opening and delete suspicious emails or attachments



Keep your software updated



INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

Introduction of Digital Security

- **Digital Security** is the protection of one's digital personality, as it represents the physical identity on the network you are operating on or the internet service in use.
- **Digital Security** includes the tools which one uses to secure his/her identity, asset and technology in the online and mobile world.

Continued..

Unfortunately, millions of people have learned the importance of digital security the hard way.

According to the Breach Level Index, more than **14 billion individual data records** have been exposed globally since 2019. That's **500+ records every second**.

As our **digital footprints** continue to grow, we can expect these numbers only to increase.

That is, unless we all brush up on personal **digital security** basics.

What info hackers are digging into?

There are three big buckets of info that hackers are digging into:

- 1- Personally Identifiable Information:** information that can be used to identify or locate you, including your name, address, phone number, date of birth, etc.
- 2- Personal Payment Information:** Information like debit card numbers, online banking credentials, checking account numbers, and PIN numbers.
- 3- Personal Health Information:** Health information is also valuable form of information for a hacker, with one record going for upward of thousands of dollars on the black market.

Things That Make You Vulnerable

- 1- Weak Passwords
- 2- Sharing passwords
- 3- Writing Your Passwords Down
- 4- Password Reset Options and Compromised Email Accounts



Analyzing Digital Threats

Analyzing Digital Threats

In today's digital age, the risks facing individuals and organizations are **constantly evolving**. With **risk assessment and analysis** people can uncover their digital and social media exposure, identify risks to their brands, business, people and locations, and walk away with a plan to better protect themselves.

In the following chart we'll learn how to identify the digital risks:

Continued..

Probability ↑	Very Likely	Acceptable Risk (medium – 2)	Unacceptable Risk (high – 3)	Unacceptable Risk (extreme – 5)
	Likely	Acceptable Risk (low – 1)	Acceptable Risk (medium – 2)	Unacceptable Risk (high – 3)
	Unlikely	Acceptable Risk (low – 1)	Acceptable Risk (low – 1)	Acceptable Risk (medium – 2)
	Ocurrence / Impact	Low	Moderate	High
Probability x Impact = Risk		Impact (how serious is the risk?) →		

Security vs Safety

Security: is the process of ensuring our safety; responsible for maintaining the safeguards we expect will always be in place. In order for security to be effective, the components of how our safety is defined need to remain unchanged.

Safety: is a state in which we are certain that our emotional and physical protection are being well taken care of.

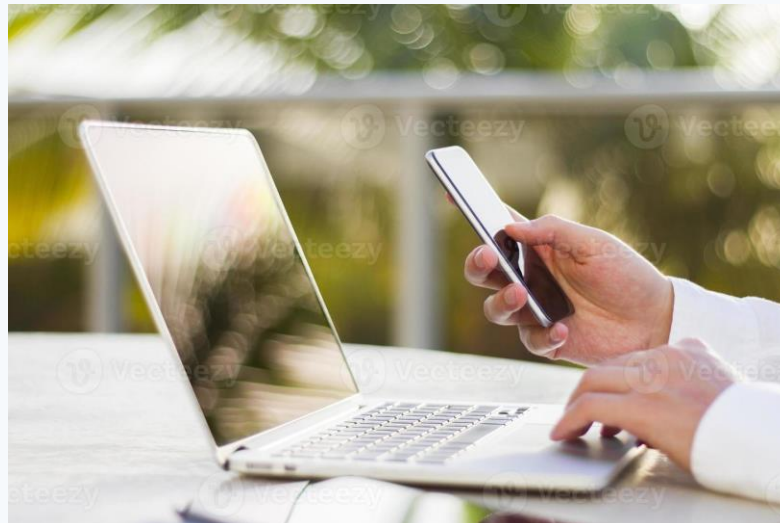


Protecting Information and Devices from Physical threats

Protection of devices from physical threats

Portable devices such as **laptops**, **phones** are particularly vulnerable to theft, loss, and resale, and should be properly secured physically.

A laptop computer or mobile phone defines convenience and mobility. It enables you to work from home, a hotel room, a conference hall, or a coffee shop.



Protection of devices from physical threats

Maybe you've taken steps to secure the data on your laptop/phone: You've installed a **firewall**. You update your **antivirus** software. You protect your information with a **strong password**. You **encrypt** your data, and you're **too smart to fall** for those emails that ask for your personal information.

But what about the laptop/phone itself?

Protection of devices from physical threats

A **minor distraction** is all it takes for your laptop to vanish. If it does, you may lose more than an **expensive piece of hardware**. The fact is, if your data protections aren't up to par, that sensitive and valuable information in your laptop may be a magnet for an identity thief.



Tips to protect devices from physical threat

Keep these tips in mind when you take your laptop out and about:

- Treat your laptop like **cash**
- Keep it **locked**
- Keep it **off the floor**
- Keep your **passwords elsewhere**
- Mind **the bag**
- Get it **out of the car**
- Don't leave it **for just a minute**



Tips to protect devices from physical threat

- **Pay attention** in airports or crowded places
- Be **vigilant** in hotels
- **Use bells** and whistles or any other alert system in place
- Know where **to turn for help**
- Keep all the **liquid away** from your devices.



Activating Windows Firewall and Updates

What is a Firewall?



What is a firewall?

Firewall is a network security, either **hardware or software based**, that uses **rules to control incoming and outgoing network traffic**.

Firewall acts as a **barrier** between a **trusted** and **untrusted** networks. Firewall controls access to the resources of network through a positive control model

Using anti-virus in a computer

What is a computer virus?

Let's first define what computer **Virus** is:

A **virus** is any unwanted program that enters a user's system without their knowledge. It can **self-replicate** and **spread**. It performs unwanted and malicious actions that end up affecting the **system's performance** and user's **data/files**. A computer virus can be thought of as an illness of the computer, just like **human viruses** that cause diseases in humans.

What is a computer ant-virus?

Now what is an **anti-virus**:

An antivirus software, as the name indicates, is a program that works **against a virus**. It **detects** or **recognizes** the virus, and then after detecting the presence of the virus, it works on **removing** it from the computer system. Antivirus software works as a **prophylactic** so that it **not only eliminates** a virus but also **prevents** any potential virus from infecting your computer in the future.

What harm can a virus do to your computer?

In case your computer is attacked by a virus, it can affect your computer in the following ways:

- Slow down the computer
- Damage or delete files
- Reformat hard disk
- Frequent computer crashes
- Data loss
- Inability to perform any task on the computer or the internet

Some of the available anti-virus software:

1- Avast

2- Bitdefender Free Edition

3- AVG

4- Kaspersky

5- Sophos Home Security

6- Panda Dome

7- Adaware

8- Comodo

9- ZoneAlarm

10- Avira

Can Macs get virus?

Can Macs get virus?

Yes, Macs can — and do — get viruses and other forms of malware. And while Mac computers are **less vulnerable** to malware than PCs, the built-in security features of macOS are **not enough** to protect Mac users against **all online threats**.

Creating very strong and secure passwords

How secure is your password?

howsecureismypassword.net

PASSWORDS & 2 FACTOR

Problem 1: People choose bad passwords



1. 123456
2. Password
3. 12345
4. 12345678
5. Qwerty
6. 123456789
7. 1234
8. Baseball
9. Dragon
10. football

PASSWORDS & 2 FACTOR

Problem 2: People store their passwords badly (because they can't remember them)



PASSWORDS & 2 FACTOR

Problem 3: People reuse passwords for many different sites which is wrong



Example of strong password:

n3Jvhdns2EgIL3bgkQsr

Password Manager

keepass.info

PC & browser cleaning and Privacy protection

Lets clean our PCs for better performance

Use ccleaner for windows:

ccleaner.com

PC and Mobile browser cleaning

The days when the internet was a series of **simple text pages** have long gone. Today's sites can contain **video**, **audio**, interactive **elements**, and stacks of **images**, and over time your browser can slow down under the weight of all that content.

With a bit of timely maintenance and tidying up, you can ensure your browsing stays faster for longer.

his advice applies across all the major desktop browsers, including Google **Chrome**, Mozilla **Firefox**, Microsoft **Edge**, Apple's **Safari**, and **Opera**.

Continued..

Before you begin clearing, your web browser's cache, cookies, and history may remove data such as the following:

- Saved passwords
- Address bar predictions
- Shopping cart contents, etc.

While you should clear your web browser's **cache**, **cookies**, and **history** periodically in order to prevent or resolve performance problems, you may wish to record some of your saved information first.

Virtual Private Network (VPN)

How a VPN works



EMSISOFT

What is a VPN?

- A **virtual private network (VPN)** extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection.

How VPNs work?

- VPNs typically allow only authenticated remote access using tunneling protocols and encryption techniques.
- The VPN security model provides
 - confidentiality such that even if the network traffic is sniffed at the packet level, an attacker would see only encrypted data
 - sender authentication to prevent unauthorized users from accessing the VPN
 - message integrity to detect any instances of tampering with transmitted messages.

Benefits of Using VPN

- **Enhanced security.** When you connect to the network through a VPN, the data is kept secure and encrypted. In this way, the information is away from the hackers' eyes.
- **Online anonymity.** Through a VPN you can browse the web in complete anonymity. Compared to hide IP software or web proxies, the advantage of a VPN service is that it allows you to access both web applications and websites in complete anonymity.
- **Unblock websites & bypass filters.** VPNs are great for accessing blocked websites or for bypassing Internet filters. This is why there is an increased number of VPN services used in countries where Internet censorship is applied.
- **Change the IP address.** If you need an IP address from another country, then a VPN can provide you this.

Digital Data Backups

What is a Data backup?



What is Data backup

Data backup is a practice that combines techniques and solutions for efficient and cost-effective backup. **Your data is copied to one or more locations**, at pre-determined frequencies, and at different capacities.

You can set up a **flexible data backup operation**, using your own architecture, or make use of available Backup as a Service (BaaS) solutions, mixing them up with local storage.

Why a Data backup is important?

In an increasingly digitized business landscape, **data backup is vital** for the survival of an organization.

You can:

- get hacked
- Ransomed
- lose your data to thieves,
- Injected malware can corrupt your hard-earned information
- Disgruntled employees or other insider threats can delete your valuable digital assets

Offline vs Cloud Data Backups

Cost



While backing up a small amount of data to the cloud is cheap, costs can escalate quickly over time as volumes grow.

On-premises hardware, especially a disk-based product, gets expensive. Disks also need to be replaced, at a faster rate than tapes.

Scalability



Cloud backups are easy to scale and there is essentially no storage limit, but be careful of cost as space increases.

In addition to a traditional backup setup, an organization needs to be wary of space, cost and the process of actually installing it.

Accessibility



Cloud backups are easy to access when you're connected to the internet. However, getting lots of data out of the cloud can take a long time.

On-premises hardware is easily accessible, unless there's a disaster at that site. Speed varies, with disk among the faster techs and tape among the slower.

Security



Increasingly less of a concern, end-to-end security will be a key feature in any top cloud backup product.

Top local backup products will have security features, but they are still susceptible to a cyberattack or a disaster at the primary site.

Management



The cloud provider typically takes care of management, which is especially helpful for businesses that don't have the resources.

IT staff will need to manage local backup. An organization may prefer its own management versus outsourcing it to a provider.

Recovery



Failing over to a cloud disaster recovery platform is a straightforward process, but actually recovering data out of the cloud can be burdensome.

It depends. If there's a disaster at the primary site, local backup probably won't be an option. For less catastrophic events, recovery can be quick.

Introduction to data recovery, Available data recovery tools

ccleaner.com/recuva

What is a digital encryption and how it works? Can emails be encrypted? If yes, how?

What is Data Encryption

Data encryption translates data into another form, or code, so that only people with access to a **secret key** (formally called a **decryption key**) or password can read it.

Encrypted data is commonly referred to as **ciphertext**, while unencrypted data is called **plaintext**. Currently, encryption is one of the most popular and effective data security methods used by organizations.

Can we encrypt emails?

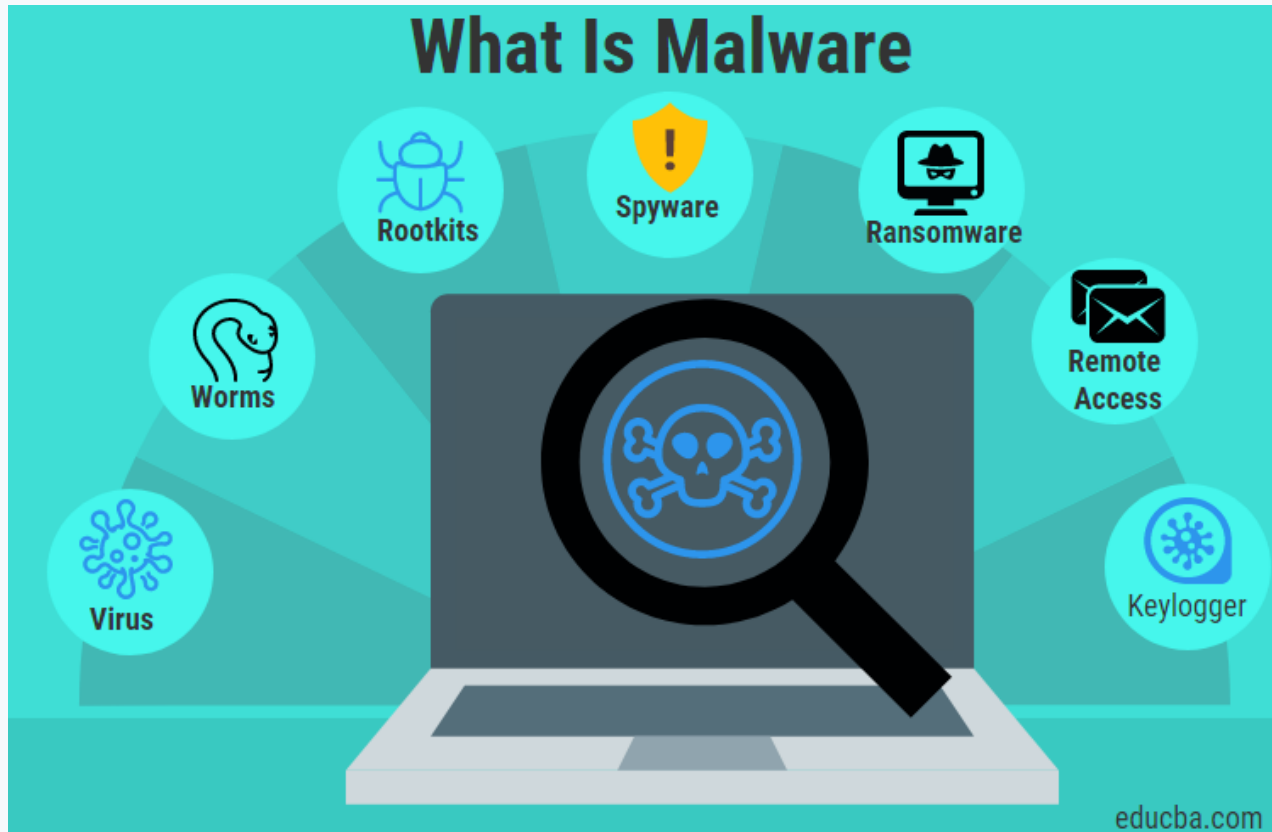
Yes, we can use this free services to do so.

<https://tutanota.com>

Protecting devices from Malware and Phishing attacks

What is Malware?

Short for "**malicious software**" malware refers to software programs designed to damage or do other unwanted actions on a computer system



Types of Malware

Type	What It Does
Ransomware	disables victim's access to data until ransom is paid
Fileless Malware	makes changes to files that are native to the OS
Spyware	collects user activity data without their knowledge
Adware	serves unwanted advertisements
Trojans	disguises itself as desirable code
Worms	spreads through a network by replicating itself
Rootkits	gives hackers remote control of a victim's device
Keyloggers	monitors users' keystrokes
Bots	launches a broad flood of attacks
Mobile Malware	infects mobile devices

How to detect phishing emails?

1. Legit companies don't request your sensitive information via email

Most companies will not send you an email asking for passwords, credit card information, credit scores, or tax numbers, nor will they send you a link from which you need to login.

2. Legit companies have domain emails

Don't just check the name of the person sending you the email. Check their email address by hovering your mouse over the 'from' address. Make sure no alterations (like additional numbers or letters) have been made


Characteristics of phishing emails

How to spot phishing:



- Seems too good to be true (Lottery!)
- Misleading URL (and URL shortners)
- Poor spelling / grammar
- Generic greeting
- Message asks for personal information
- You did not initiate the action
- Something doesn't look right!
- Unrealistic threats especially from security agencies or banks
- You are asked to send money to cover expenses

Continued..

From: GlobalPay <VT@globalpay.com> 
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

[Hide](#)

1 Attachment, 7 KB

Save ▼

Quick Look

Dear customer,

We regret to inform you that your account has been restricted.

To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc



[update2816.html \(7 KB\)](#)

Notice the generic salutation at the beginning, and the unsolicited web link attachment?

805

[Alert] Your account has been locked for security reason!

Today at 11:42 AM



Hello,

Your Apple ID has been temporarily locked because we unable to verify your billing information on your account.

If you do not update your information in 24 hours, your Apple ID will be permanently locked. To continue to enjoy Apple ID benefits, please visit this link to log in to your Apple ID and update your billing information.

<https://appleid.apple.com/update/billing>



Apple To: cs-noreply.mail@automatedapplemail.com

2:25 PM

[Reminder] Your account has been locked for security reason!



Your accounts has been changed!

Dear Customer,

We've noticed your password on Apple account successfully changed. But, we've detected your account was accessed without your permit. For security reason your account has been locked.

We need your help for unlock your account. Please help us to unlock your account with click the button below and verify your identity. Your account will became locked until you verify your identity.

Unlock My Account

If you do not verify your account within 24 hours we will disable your account and all service permanently.

Copyright ©2020 Apple, Inc.



What should you do when you receive a phishing email?

- Contact the person who sent it (Social distancing)
- Inform IT personnel
- Share **screenshot** to create awareness
- Mark as phishing email
- Block sender . Do not respond!
- Delete

Social Media and how to deal with trolls, bots, hate speech in Social Media

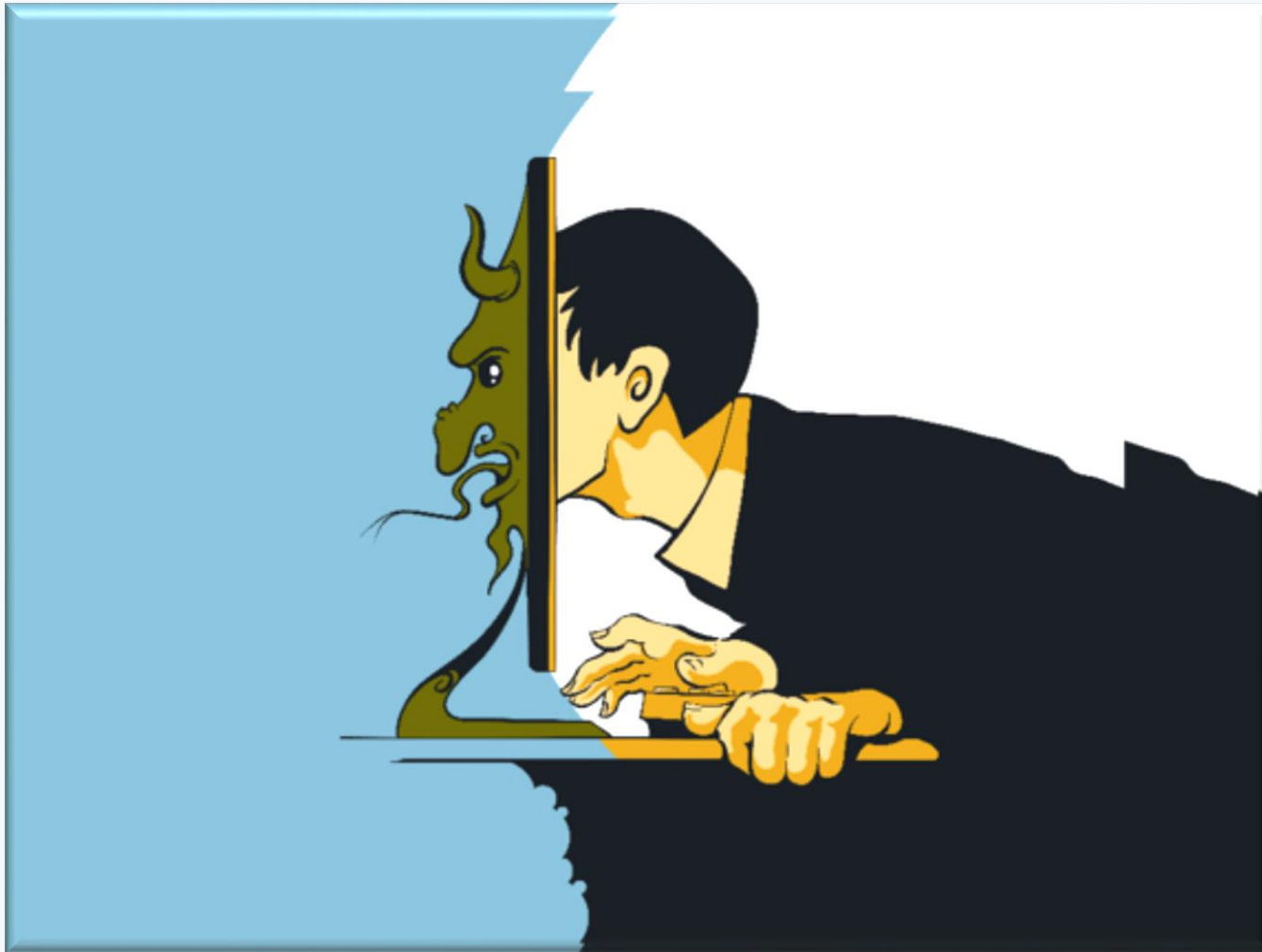
The Social Media



KAYS FITTINGS

**How many social media
platforms you use?**

What can you understand from this photo?



What are Social Media trolls?

They are people who deliberately provoke others online. By saying inflammatory, negative and offensive things. They live to make people upset and angry.

Continued..

They rant, post death threats, spew hate speech. They attack an opponent's character. And say things to appeal to people's feelings (rather than their intellect).

Who are they?

They can be your fans and followers or other strangers

How to deal with trolls?

1- Respond Respectively

2- Ignore:

3- Delete & Block:

4- Find support group

Presenter's Personal Information

Name: Abdifatah Ali Mohamud

Signal/WhatsApp: +252-615180908



Personal Email: farayare100@gmail.com

Twitter handle: @thefarayare