DIGITAL SAFETY AND SECURITY

for Educators in times of the Pandemic

Encrypt
UGANDA

INTRODUCTION

1. ABOUT ENCRYPT UGANDA

- Provides protection measures to the ever-increasing digital security threats, security assessments, privacy, developing and analyzing digital tools.

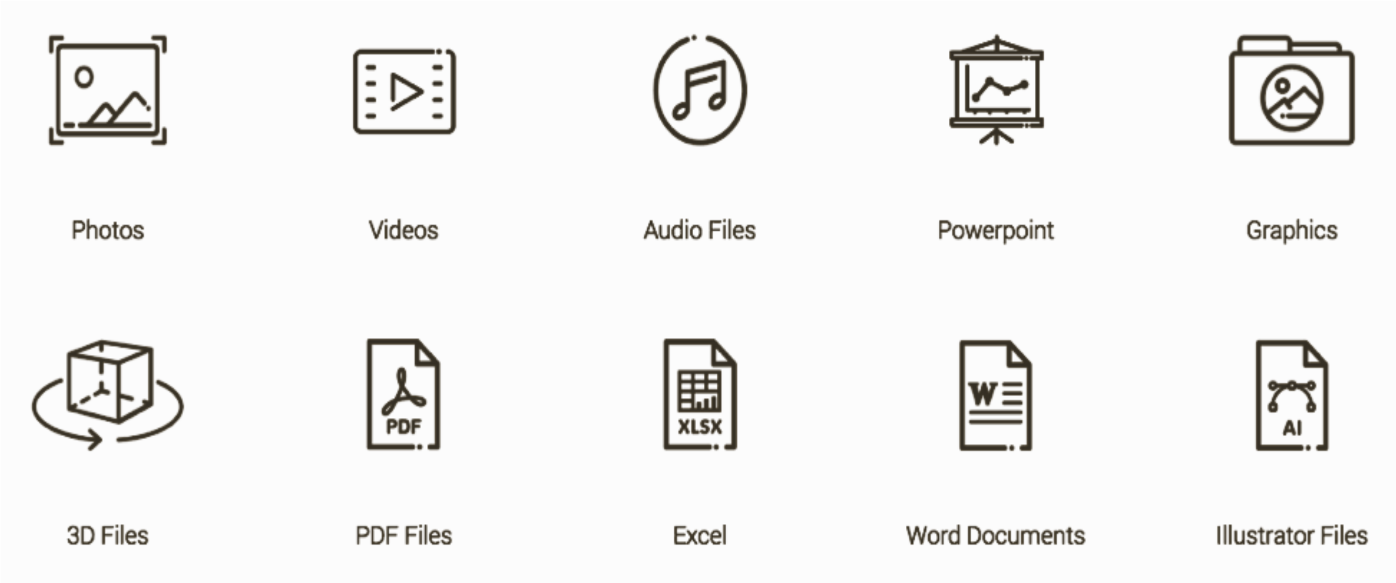
2. THE TEAM PRESENT

- Gole Andrew
- Senfuma Bryan Kaye

What is digital security?

Digital security is the protection of computer systems and data from unauthorised use or harm.

1: What Digital Assets are you protecting?



- Photos
- Videos
- Audio Files
- Powerpoint
- Graphics
- 3D Files
- PDF Files
- Excel
- Word Documents
- Illustrator Files

TYPES OF THREATS

- Malware
- Virus
- Spyware
- Adware
- Ransomware
- Phishing
- Hacking
- Worms
- Trojans
- Hoax
- Spam
- Keylogger
- Identity theft
- Man in the middle

Phishing

Phishing: Is the fraudulent attempt to obtain sensitive information such as usernames and passwords by posing as a legitimate person or entity.

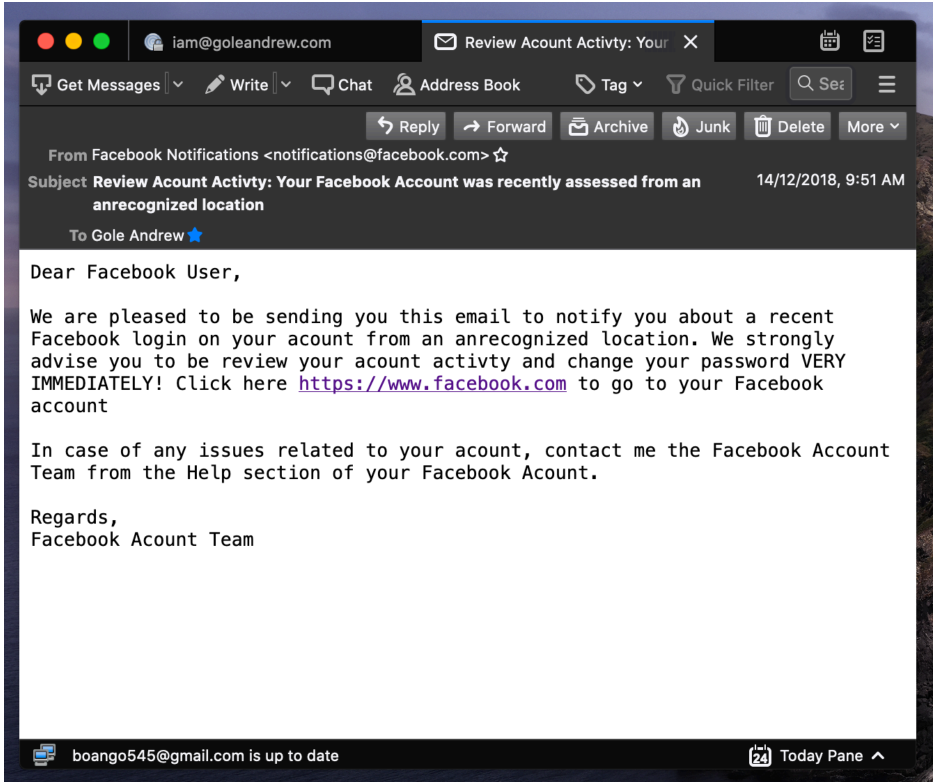
How to Identify Phishing Attacks

- Emails with generic greetings
- Emails requesting personal information.
- Emails requesting an urgent response
- Emails with spoofed links.

VIDEOS ON PHISHING AND PHARMING

https://www.youtube.com/watch?v=_3hK0PuSkhw
https://www.youtube.com/watch?v=BnmneAjVrM4

Example of a Phishing Email



From Facebook Notifications <notifications@facebook.com>

Subject **Review Acount Activty: Your Facebook Account was recently assessed from an anrecognized location** 14/12/2018, 9:51 AM

To Gole Andrew

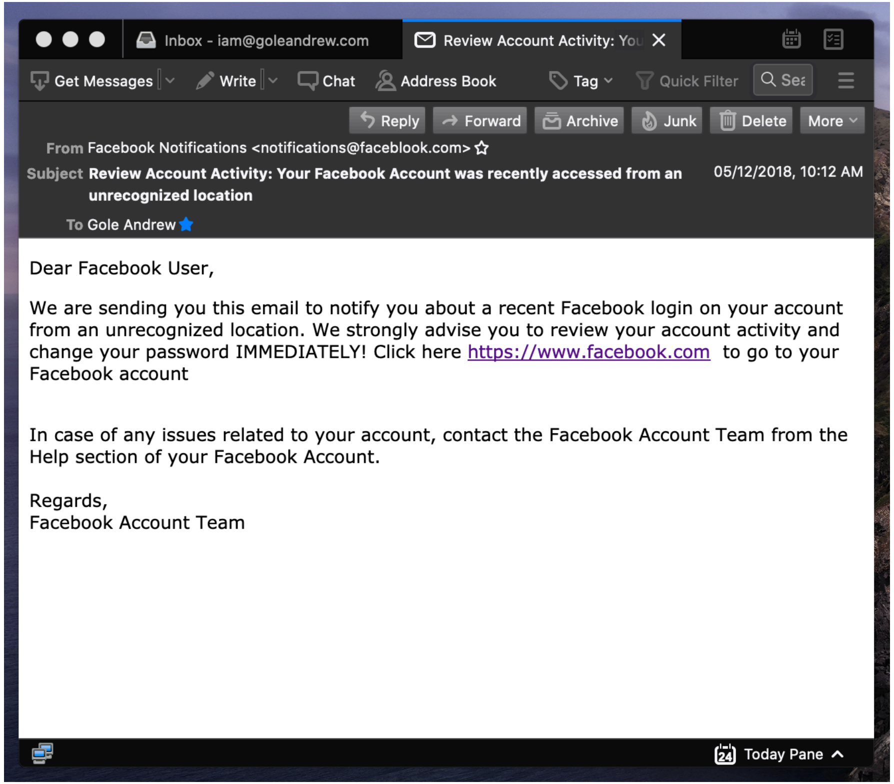
```
Dear Facebook User,

We are pleased to be sending you this email to notify you about a recent
Facebook login on your acount from an anrecognized location. We strongly
advise you to be review your acount activty and change your password VERY
IMMEDIATELY! Click here https://www.facebook.com to go to your Facebook
account

In case of any issues related to your acount, contact me the Facebook Account
Team from the Help section of your Facebook Acount.

Regards,
Facebook Acount Team
```

boango545@gmail.com is up to date



From Facebook Notifications <notifications@faceblook.com>

Subject **Review Account Activity: Your Facebook Account was recently accessed from an unrecognized location** 05/12/2018, 10:12 AM

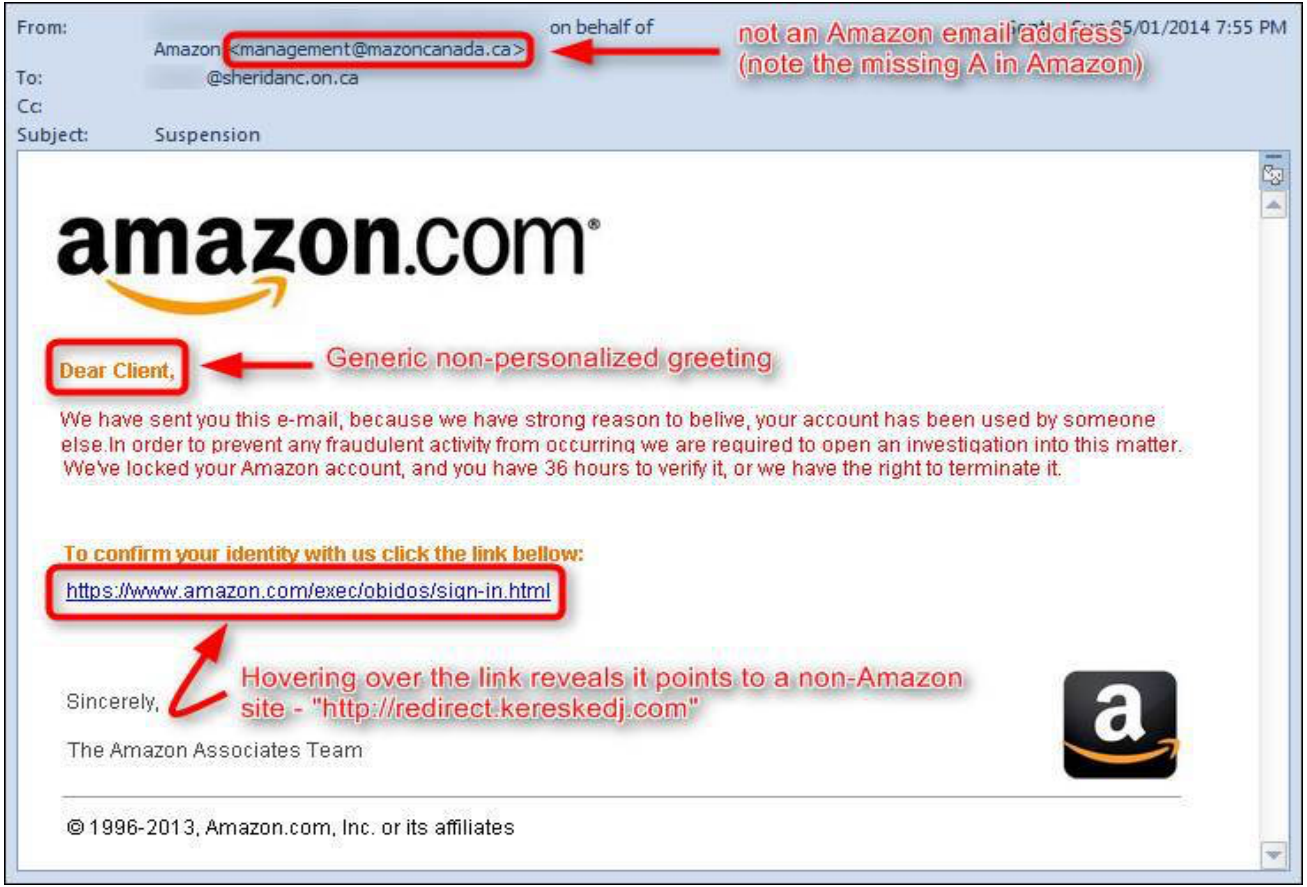
To Gole Andrew

Dear Facebook User,

We are sending you this email to notify you about a recent Facebook login on your account from an unrecognized location. We strongly advise you to review your account activity and change your password IMMEDIATELY! Click here https://www.facebook.com to go to your Facebook account

In case of any issues related to your account, contact the Facebook Account Team from the Help section of your Facebook Account.

Regards,
Facebook Account Team



From: [redacted] on behalf of Amazon <management@mazoncanada.ca> Sent: Sun 05/01/2014 7:55 PM

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Steps to mitigate phishing

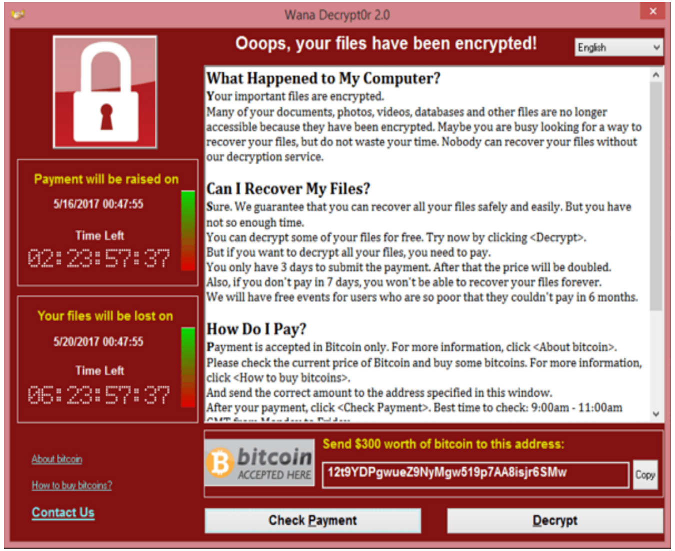
- Verify every email sender’s address
- Confirm sender’s identity if unsure
- Report suspicious activity to technical teams
- Don’t open email attachments from unknown senders
- Think twice: Don’t click on links in suspicious emails
- Double check especially if the email is about sending money, bank details or sensitive information

Ransomware

Ransomware is a type of malware that encrypts a victim's files, holding them hostage unless the victim pays a ransom for their decryption.

How to Identify Ransomware attack

- The files will be encrypted
- A ransom message will always be displayed on



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How to guard against Ransomware attacks

- Back up your data on a regular basis
- Keep all your software up-to-date
- uninstalling any unnecessary services and software
- Scan networks for risky accounts using weak passwords
- Install an anti-malware software

HANDS ON

DATA PROTECTION

Encrypt
UGANDA

FORMS OF DATA

Data at Rest

- data stored on a hard drive, laptop, flash drive among other storage mediums

Data in Transit

- is data actively moving from one location to another such as across the internet or through a private network.

Encrypt
UGANDA

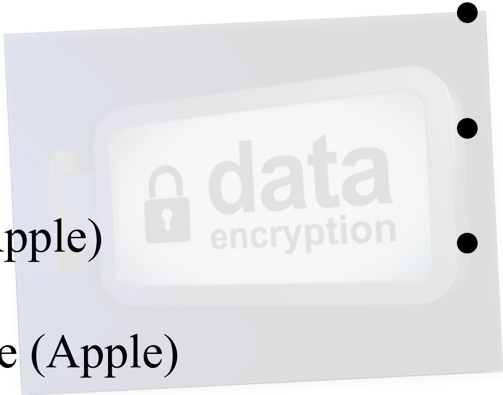
Best Practices for Data Protection

		Data at Rest	Data in Transit
1	Backup critical data	✓	✗
2	Lock your computer every time you step away from it	✓	✗
3	Keep your software and system up-to-date	✓	✗
4	Use strong passwords	✓	✓
5	Install an anti-malware	✓	✓
6	Overwrite deleted file	✓	✗
7	Train and educate your team	✓	✓
8	Encrypt your data	✓	✓

Encrypt UGANDA

Data encryption and backup tools Tools

- BitLocker
- VeraCrypt
- FileVault2 (Apple)
- Time Machine (Apple)



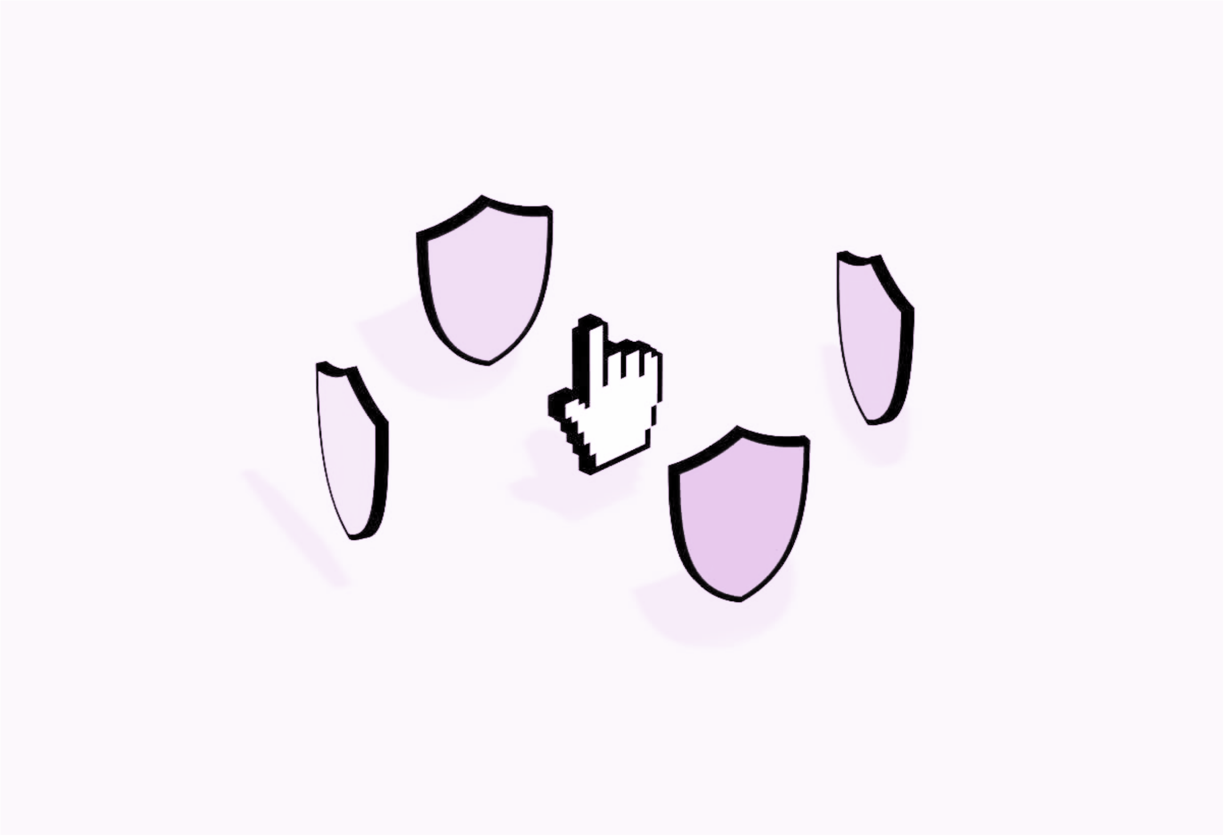
- Google drive sync
- iCloud
- Dropbox

Encrypt
UGANDA

ONLINE SECURITY

- Safe browsing
- Social media safety
- Email security

Safe web browsing



What is a web browser?

It is a program you use to view websites on the Internet. E.g Chrome, Firefox, Safari, microsoft edge etc..

How can we protect our web browsing?

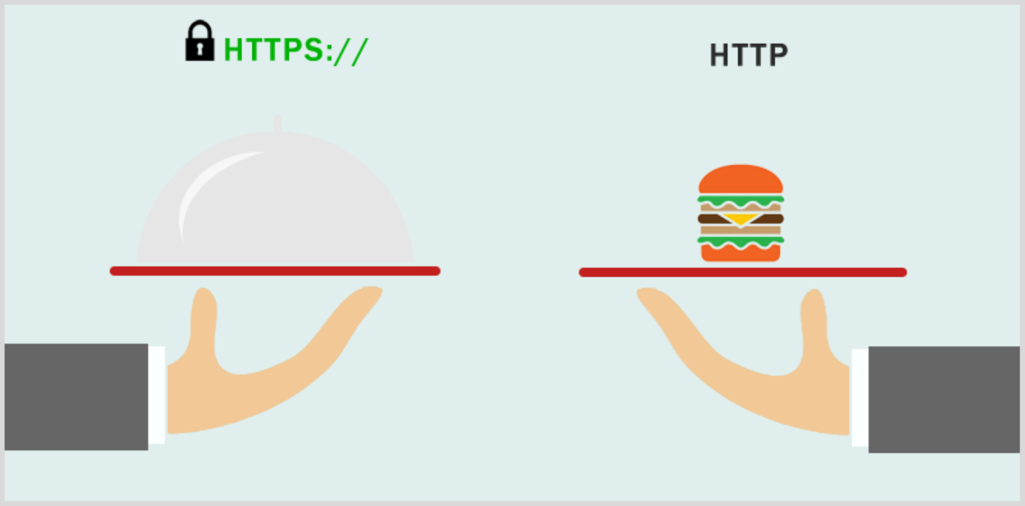
- Customise your security settings
- Use a VPN to hide your identity
- Update your software
- Never store passwords in your browser
- Block Pop-ups and scripts

Encrypt UGANDA

HTTP Vs. HTTPS

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure



HTTPS is far more secure than HTTP. A website that uses HTTP has http:// in its URL, while a website that uses HTTPS has https://.

Encrypt UGANDA

Web browser security extensions

- ***HTTPS EveryWhere***

-Its allows you get HTTPS connections on most of the sites

- ***Avast Online security***

-Detect dangerous sites -Protect against phishing scams

- ***Privacy Badger***

-Block sites that try to track your browsing habit

- ***Click and clean***

-Used to clear traces of your online activity

- ***Adblock plus***

-Blocks adverts in your web browser

SOCIAL MEDIA SAFETY

Social Media Essentials

Encrypt
UGANDA

1. Security Features and Privacy Settings:

Connection Security

Does the social media site provide a connection over SSL. If it doesn't, your content can be seen as it is sent between you and the internet.

Privacy Features

-What privacy options are provided for users? - Is all of your information available to those with an account? - Can you choose to share personal data or shared content securely with a small number of users? Or is it shown to all users by default?

Location Tracking

What Are You Choosing to Share?

When you share information you might be making information available about yourself and others to people who want to abuse or misuse it.

Who are your friends?

Do you know all these people? Do you trust them with everything you post online that they can see? Don’t accept “friend” or contact requests easily. In particular, ask yourself:

EMAIL SECURITY

EMAIL SECURITY

Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.

The Need for Email Security

- Protect confidential information
- Avoid identity theft
- Phishing
- Malware

Email Security Best Practices

1 Use email encryption for both email content and attachments

2 Never open attachments or click links from unknown senders

3 Never share your password including co-workers

4 Use spam filters and an anti-virus software

5 Change password often and use best practices for creating them

6 Implement a data protection solution to identify sensitive data and prevent it from being lost via email

7 Be sure to log out everytime you sign into your account

8 Use a different password for each of your accounts

9 Learn how to recognise phishing

10 Always check your email activity and settings

PASSWORD MANAGEMENT AND 2 STEP VERIFICATION

Encrypt
UGANDA

Challenges in password management

1. Login spoofing
2. Sniffing attack:
3. Shoulder surfing attack
4. Brute force attack
5. Phishing attack

Traditional methods of password management

- Writing down passwords on sticky notes, note books, etc.
- Sharing them via spreadsheets, email, telephone, etc.
- Using simple and easy to guess passwords
- Reusing them for all web applications

Examples of weak passwords

- Any word that can be found in a dictionary (e.g security , mother..etc).
- A dictionary word with some letters simply replaced by numbers (e.g., a1rplan3 or aer0plan0).
- A repeated character or a series of characters (e.g., AAAAA, ABCDor 12345).
- Personal information (names of your kids/friends,birthdays…..etc).
- Anything that’s written down and stored somewhere e.g near your computer.

What makes a strong password

1 It should be Unique

2 Should be Very Long

3 Should be Fresh

4 Should be Practical

5 Should be Impersonal

6 It should be a Secret

7 A mixture of upper and lower case letter, numbers and special characters

Checking Strength of your Password:

https://www.security.org/how-secure-is-my-password/

Encrypt UGANDA

Password Managers

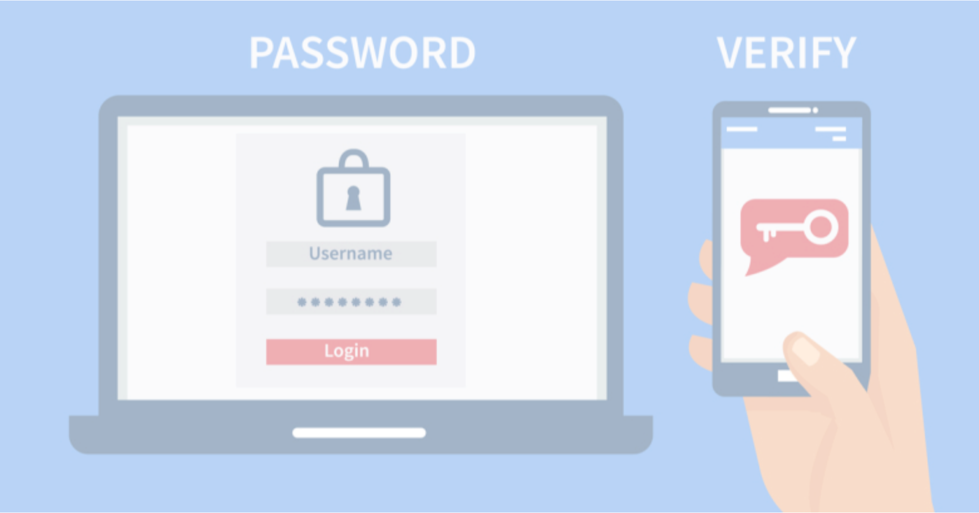
A password manager is a digital vault that stores your login credentials.

Examples:

- Keepass
- LastPass

2 Factor Authentication/Verification

is an extra layer of protection used to ensure the security of online accounts beyond just a username and password.



MOBILE SECURITY

Mobile phone protection

- Use a passcode
- Keep software up to date
- Write down your IMEI
- Enable remote wiping
- Enable mobile encryption
- Backup your phone regularly
- Turn Off inactive bluetooth
- Be selective with your applications
- Install mobile anti-malware
- Connect to secure WIFI and use a VPN
- Completely wipe all data on the phone before disposal

Secure mobile applications

- Signal
- Silence
- WhatsApp

General digital security tips

- Think before you download software and stay up-to-date
- Use unique and complex passwords
- Use a password manager
- Enable 2-factor authentication on all your accounts
- Use end-to-end encrypted communication tools
- Encrypt your hard drive and phone
- Choose the right web browser and security settings
- Detect and prevent phishing attempts
- Encrypt and backup your data

General digital security tips

- Anti-malware protection is a must
- Don't store passwords with your laptop or mobile device
- Set your device to automatically lock after a period of inactivity
- Don't use the same password for more than one account or service
- Develop a security plan
- Always register and assess each threat you face
- Never leave your devices unattended to

“For every lock, there is someone out there trying to pick it or break in”

David Bernstein

THANK YOU

Encrypt
UGANDA