DIGITAL SAFETY AND SECURITY for Educators in times of the Pandemic
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: 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

Dear Facebook User,

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

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

Regards,
Facebook Account Team
Dear Client,

We have sent you this e-mail, because we have strong reason to believe, 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 below:
https://www.amazon.com/exec/obidos/sign-in.html

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
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
DATA PROTECTION
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.
# Best Practices for Data Protection

<table>
<thead>
<tr>
<th></th>
<th>Data at Rest</th>
<th>Data in Transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Backup critical data</td>
<td>✔️</td>
</tr>
<tr>
<td>2</td>
<td>Lock your computer every time you step away from it</td>
<td>✔️</td>
</tr>
<tr>
<td>3</td>
<td>Keep your software and system up-to-date</td>
<td>✔️</td>
</tr>
<tr>
<td>4</td>
<td>Use strong passwords</td>
<td>✔️</td>
</tr>
<tr>
<td>5</td>
<td>Install an anti-malware</td>
<td>✔️</td>
</tr>
<tr>
<td>6</td>
<td>Overwrite deleted file</td>
<td>✔️</td>
</tr>
<tr>
<td>7</td>
<td>Train and educate your team</td>
<td>✔️</td>
</tr>
<tr>
<td>8</td>
<td>Encrypt your data</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Data encryption and backup tools

- BitLocker
- VeraCrypt
- FileVault2 (Apple)
- Time Machine (Apple)
- Google drive sync
- iCloud
- Dropbox
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
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://.
Web browser security extensions

- **HTTPS EveryWhere**
  - Allows you to 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
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 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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Use email encryption for both email content and attachments</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Never open attachments or click links from unknown senders</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Never share your password including co-workers</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Use spam filters and an anti-virus software</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Change password often and use best practices for creating them</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Implement a data protection solution to identify sensitive data and prevent it from being lost via email</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Be sure to log out everytime you sign into your account</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Use a different password for each of your accounts</td>
</tr>
<tr>
<td><strong>9</strong></td>
<td>Learn how to recognise phishing</td>
</tr>
<tr>
<td><strong>10</strong></td>
<td>Always check your email activity and settings</td>
</tr>
</tbody>
</table>
PASSWORD MANAGEMENT
AND 2 STEP VERIFICATION
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**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>It should be Unique</td>
</tr>
<tr>
<td>2</td>
<td>Should be Very Long</td>
</tr>
<tr>
<td>3</td>
<td>Should be Fresh</td>
</tr>
<tr>
<td>4</td>
<td>Should be Practical</td>
</tr>
<tr>
<td>5</td>
<td>Should be Impersonal</td>
</tr>
<tr>
<td>6</td>
<td>It should be a Secret</td>
</tr>
<tr>
<td>7</td>
<td>A mixture of upper and lower case letter, numbers and special characters</td>
</tr>
</tbody>
</table>

**Checking Strength of your Password:**

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