INFORMATION SECURITY

Instructor: Charles Kasamba

RSCE/ICTS/ICT Security

Date: October 2017

Location: Entebbe, Uganda

Scope of Training

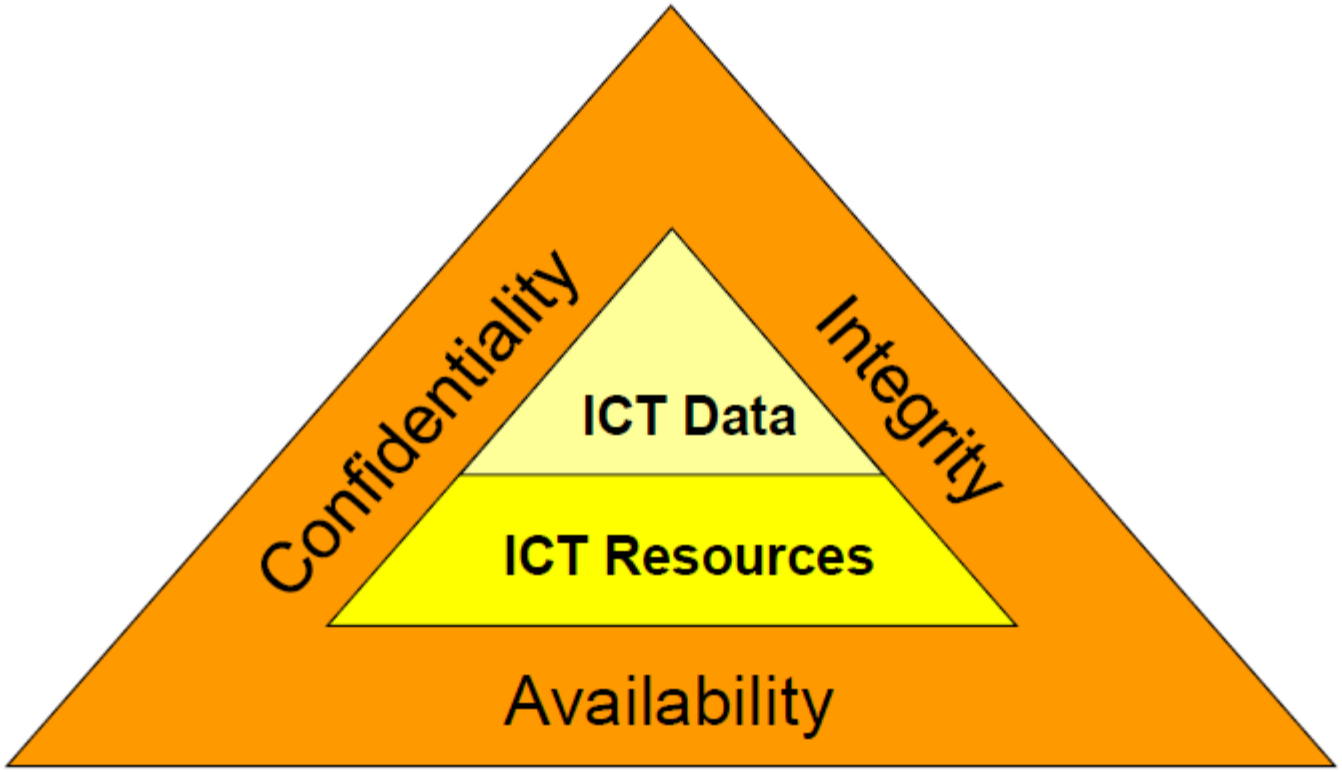
- Purpose of Information Security
- Information Threats and Classification
- Social Engineering
- Password Protection
- Electronic Messaging and Phishing
- Safe Web Browsing
- Incident Response

Why Information Security ?

- Protect organization Information and Data
- Protect ICT Resources
- Protect Organization Reputation
- Protect Security of colleagues
- Protection from Intruders or Cyber Criminals

Information Security Core Purpose

Information Security Core Purpose



Key Threats to Information

- Physical and environmental threats
- External Hackers or Organizations
- Third Party relationships
- Natural Disasters
- Internal or insider leaks

Information Classification

1. Strictly Confidential
2. Confidential
3. Unclassified
4. Public

Social Engineering

- What is Social Engineering?

- What is a Social Engineering Attack?

FACT: Sometimes the Easiest Way for scammers to gain access or information is to ask for it

P@33w0rD!

- Should be Strong
- Length and Complexity
- Should be different from default or initial password
- Should be different from your username
- Should comprise of at least 3 of character classes:

example: Information (weak)

1nForm@Ti0n (strong)

- Avoid Dictionary Words, Personal information

P@33w0rD! – How to Create a Strong Password

- Insertion Based Password Creation
  - building

- Phrase Based Password Creation
  - “this is me”

P@33w0rD! – How to Protect it

- Never Share your Password
- Never include Password in email or electronic file
- Never document passwords e.g. Plaintext file, **********
- Regularly change your passwords
- Do Not enable ‘Remember Me’ functionality
- Make it Lengthy and Complex
- Use different passwords for different accounts

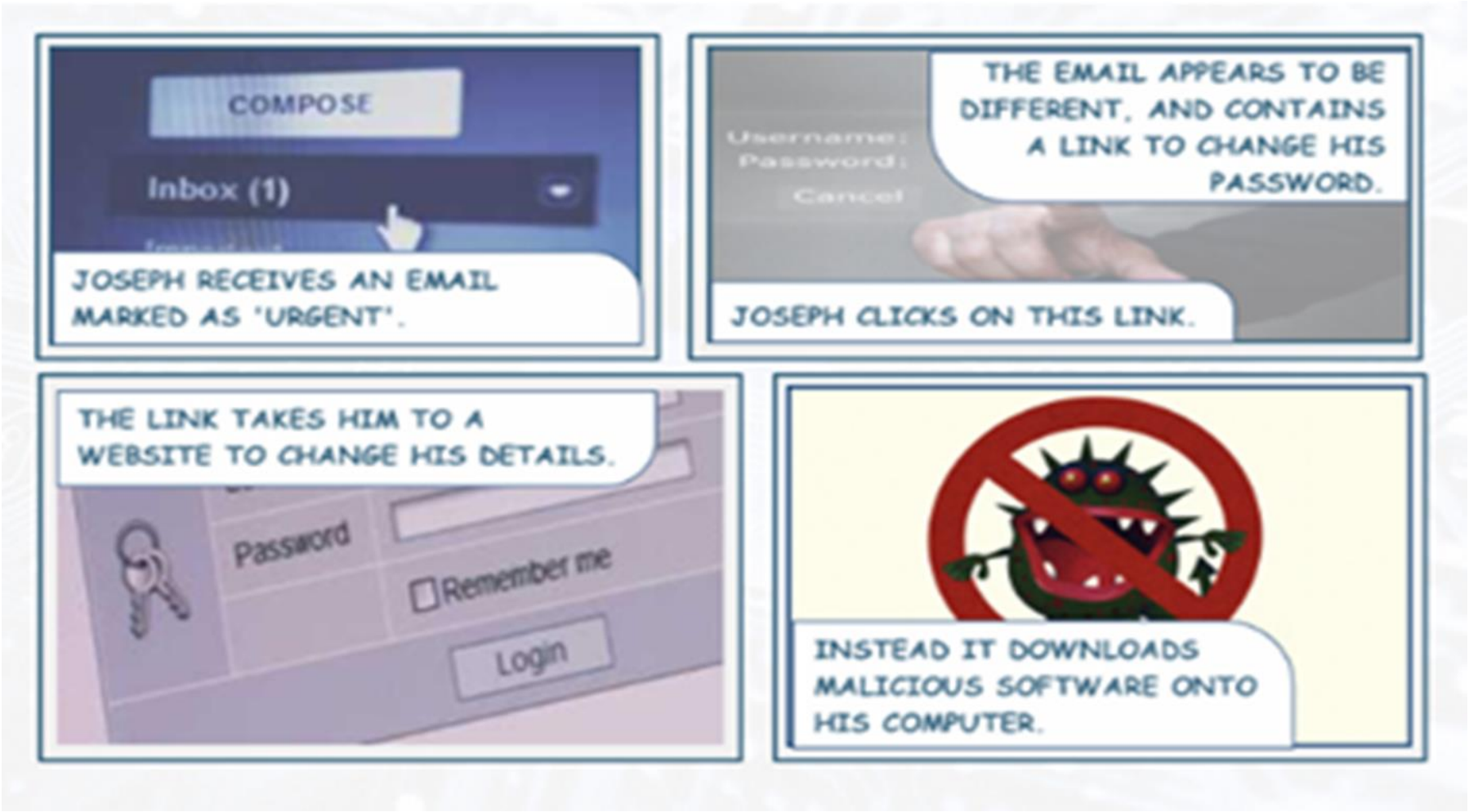
Electronic Messaging and Phishing

- Human nature can be weakest link
- No. 1 attack method for cyber criminals
- Personal email is susceptible to phishing email
- Attacks through malicious attachments, malicious links, Data capture screens.

Phishing – warning signs

- Suspicious Text
- Urgency
- Wrong or False URL's or Links
- Incorrect grammar or text that is inconsistent with usual messaging

Phishing – Scenario!



Best Practices of Email Use

STOP, THINK , CLICK!!

- Check URL correspondence to known and reputable website
- Hover over URL before clicking
- Check the sender's address is legitimate
- Report any suspicious emails
- Click on URLs only if you trust originator
- Only give your email to trusted persons
- Don't forward suspicious warning messages or emails to colleagues
- Only join chat groups and email lists when there's a business need

Safe Web Browsing!

Internet Usage Best Practices: Why?

- Computer Compromise often results from User browsing activities
- Increased sophisticated web-based attacks
- Protection of Organization Data and Information

Safe Web Browsing!

To browse the internet safely, it is important to understand how users, browsers and web sites interact.

A **browser** is a program that allows you to visit websites and search the internet
- Internet Explorer, Firefox, Chrome

A **URL** is the web address of the site you are visiting
- https://google.com
- https://cnn.com

A **website** is a set of related web pages served from a single web domain serving code and media that may interact with the browser.

Safe Web Browsing!

Risk
Attacker intercepting your information

Control
Ensure that where confidential information is communicated over the internet that the website address starts with https.

Safe Web Browsing!

Internet Usage Best Practices: Do's

- Know company acceptable use policies
- Communication within context of assigned responsibilities
- Information Sharing related to role
- Participation in educational/development activities

Safe Web Browsing!

Internet Usage Don’ts:

- Unsolicited mass mailings
- Access to Pornographic Sites
- Illegal and unlawful purposes
- Gaming
- Competitive Commercial Activity
- Dissemination of chain letters
- Peer-to-peer networks
- Uploading/downloading large data
- Introducing or distributing Malware

Incident Response

Information Security Events.

- Compromised Account
- Lost or stolen computers
- System downtime
- Policy Violations
- Malicious Software
- Unauthorized access

Incident Response

Information Security Events Indicators

- Anti-Virus Alert
- System Performance reduction
- Blocked Access
- File deletion
- Abnormal emails or attachments
- Reduced Connectivity
- Clicking or responding to phishing email
- Unauthorized bank activity
- Large spam email volumes from your account
- Unauthorized posts on your social media account

Incident Response

Information Security Events Response

- Confirm Event is security related
- Escalate to local Service Desk
- Do Not remediate solution on your own
- Change Personal Passwords
- Disconnect Laptop from internet/network
- Run software Anti-virus clean
- Contact Bank/financial institute
- Notify contacts not to open suspicious emails from you

Information Security Quiz

1. Which of the following is a good way to create a Password?

- ❑ Your children's or pet's names
- ❑ Using any letters and numbers as long as the password is five characters long
- ❑ A combination of upper and lowercase letters mixed with numbers and symbols
- ❑ Your phone number and name combined

Information Security Quiz

2. Which of the following would be the best Password?

- mySecret
- Dp0si#Z$2
- abc123
- keyboard
- Passw0rd

Information Security Quiz

3. Because I work in a secure building, I can discuss confidential information in an open work area?

- ☐ True
- ☐ False

Information Security Quiz

4. What indicated you are shopping online in a secure manner?

- I know the company
- They are selling quality goods of famous brands
- There's a banner on the top of the page saying "Secure Website"
- The URL/address of the website starts with https://...
- All of the above

Information Security Quiz

5. When travelling with a laptop you should …..

- Check in the laptop bag with your other luggage
- Stow it in the overhead bin until landing
- Keep it in your lap or at least between your feet at all times
- Hand it to a neighbor while your get settled

Information Security Quiz

6. Information Security is the responsibility of

- Information Services
- All employees
- Key employees handling sensitive or criminal justice data
- All of the above
- None of the above

Information Security Quiz

7. What can I do to reduce potential security threats?

- Do not share my password
- Turn off a computer's Antivirus Software
- Log out when I step away from my computer
- All of the above

Information Security Quiz

8. In what circumstances is it appropriate for an IT staff member to request for your password?

- ❑ To confirm that the account is disabled and no other reason
- ❑ For technical troubleshooting and no other reason
- ❑ For account verification
- ❑ Never

Information Security Quiz

9. What is/are the general cause(s) of unethical/illegal Computer Use behavior?

- Accident
- Intent
- Ignorance
- All of the above

Information Security Quiz

10. If you notice there has been a breach of non-public information, you should:

- Take notes and wait to see if there are any additional attempts to get information
- Report the incident immediately to the Information Security Officer/ or management
- Contact the local police department
- Initiate investigations into the breach

You think information security is someone else's responsibility?

Think again !!

Ignorance

Is Not Bliss

Questions?