PLATINUM
CREDIT LTD
There when you need us

Introduction to Computer Security

What is Computer Security?

Computer Security is the protection of computing systems and the data that they store or access

Why is Computer Security Important?

Computer Security allows the Business to carry out its mission by:

●Enabling people to carry out their jobs, education, and research

●Supporting critical business processes

●Protecting personal and sensitive information

Why do I need to learn about Computer Security?

Isn’t this just an IT Problem?

No this is wrong assumption Good Security Standards follow the “90 / 10” Rule:

> ***Only 10% of security safeguards are technical***
>
> ***90% of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices***

Example: Technical can put lock on the door which is like 10% of security. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90% of security. Both parts need to participate for effective security.

What Does This Mean for Me?

- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, devices and data secure.

➢*Information Security is everyone's responsibility*

- Learn **"good computing security practices."**
- Incorporate these practices into your everyday routine. Encourage others to do so as well.
- Report anything unusual – Notify your supervisor and the ITS Support Center if you become aware of a suspected security incident.

The Internet can be a hazardous place:

How many attacks to computers on financial institutions do you think take place everyday?

Hundreds Thousands of attacks per minute bombard different network on the internet.

An unprotected computer can become infected or compromised within a few seconds after it is connected to the network.

"They will just keep finding new ways to break in!"

A compromised computer is a hazard to everyone else, too – not just to you.

Quiz: A hacked computer can be used

to... (select all that apply)

a) Record keystrokes and steal passwords.

b) Send spam and phishing emails.

c) Harvest and sell email addresses and passwords.

d) Access restricted or personal information on your computer or other systems that you have access to.

e) Infect other systems.

f) Hide programs that launch attacks on other computers.

g) Illegally distribute illegal content.

h) Generate large volumes of traffic, slowing down the entire system.

i)Denial of service for proper user of the system and cause shutting down of normal business operation

j)Leaking of business confidential information to non affiliated entity with purpose to harm the business

Of course, the answer is "All of the above."

A compromised computer can be used

for all kinds of surprising things.

Many cyber security threats are largely avoidable. Some key steps that everyone can take include (1 of 2):

- Use good, cryptic passwords that can’t be easily guessed - and keep your passwords secret
- Make sure your computer, devices and applications (apps) are current and up to date
- Make sure your computer is protected with up-to-date anti-virus and anti-spyware software
- Don’t click on unknown or unsolicited links or attachments, and don’t download unknown files or programs onto your computer or other devices
- Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept
  - ➢ *To help reduce the risk, look for “https” in the URL before you enter any sensitive information or a password (the “s” stands for “secure”)*

➢*Also avoid standard, unencrypted email and unencrypted Instant Messaging (IM) if you’re concerned about privacy*

- Visit the link below to see ITS' Top 10 List and the other links on the training page for more.

➢*Top 10 List: http://its.ucsc.edu/security/top10.html*

➢*http://its.ucsc.edu/security/training/index.html#cs*

What are the consequences for security violations?

- Risk to security and integrity of personal or confidential information. e.g. identity theft, data corruption or destruction; lack of availability of critical information in an emergency, etc.
- Loss of valuable business information
- Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports
- Costly reporting requirements in the case of a compromise of certain types of personal, financial data
- Internal disciplinary action(s) up to and including termination of employment, as well as possible penalties, prosecution and the potential for sanctions / lawsuits

Please try to find out more on ITS' Security

"Remember is 90% comes from you as user"

GETTING HELP:

If you have questions, please contact the ITS Support Desk:

- ➢Kelvin Nonge
- ➢Phone : 0677 008558

Email: kelvin@platinumcredit.co.tz

- ➢Skype : kelvinjuliusnonge