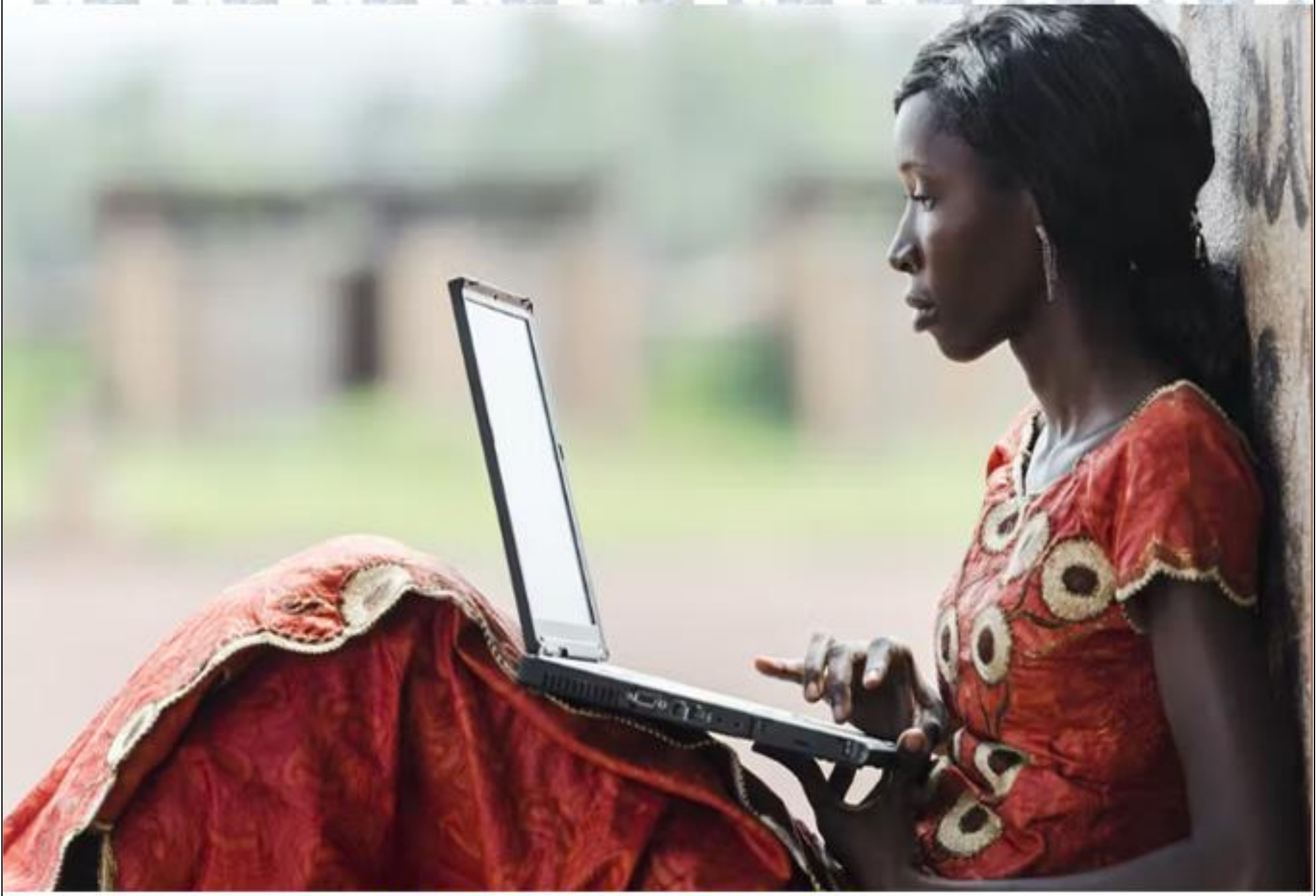
SCAMS ON THE RISE AS CYBERCRIME BOOMS



WWW.ZCSI-FOUNDATION.ORG
ZCSIF 2022

RESEARCH JOURNAL VOL 2

TABLE OF CONTENT

Abstract

Cybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet user's personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information.

What is Cybercrime?

Cybercrimes are broadly defined as any illegal activity that involves computers and other digital devices or a computer network. Including threats like social engineering, software vulnerability, exploits and network attacks. Furthermore, criminal acts like harassment, extortion, money laundering and more. Cybercrimes are costing companies and individuals billions annually, O evolution of technology and increasing accessibility of smart devices means there are multiple access points within users' homes for hackers to exploit and come up with new skill set on how they'll scam, hack someone or company. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

Categories of Cybercrime

Cybercrimes can be categorized in three types as follows:

- Property:
  Many are still falling prey to phishing links, a real life situation that happens when an attacker sends you a link, once clicked he/she has illicit information about you could be bank and credit card details.

- Individual:
  This form of Cybercrimes is an individual sending unpleasant, malicious or illegal information online. This can be Pornography, Cyberstalking.

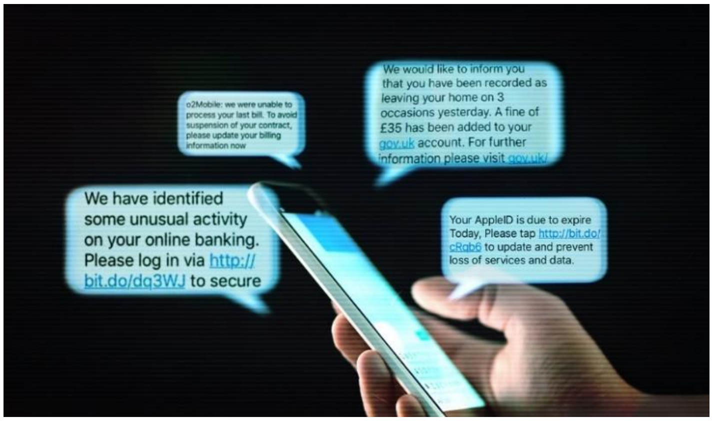
- Government:

  This is a least common Cybercrime hence the most serious one, crimes against the Government are referred to as Cyber terrorism. Distributing propaganda and having access to Government websites without consent is a serious crime.

Types of Cybercrimes

- Phishing
  Is a type of social engineering where an attacker sends fraudulent message designed to trick a victim into revealing sensitive information Users are tricked into emails claiming, need to change their password or update their billing information hence giving criminals access.

Example of phishing



o2Mobile: we were unable to process your last bill. To avoid suspension of your contract, please update your billing information now

We would like to inform you that you have been recorded as leaving your home on 3 occasions yesterday. A fine of £35 has been added to your gov.uk account. For further information please visit gov.uk/

We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure

Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.

Preventive measures

- Keep updated to the latest Phishing scams
- Think twice before clicking
- Install anti phishing
- Use a firewall
- Never give out personal information

- ## Online Scams

  These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information

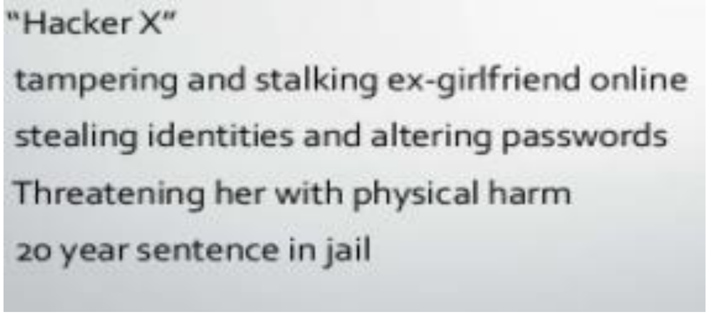
Do not send money to someone you met online, for any reason. If your online sweetheart asks for money, you can expect it is a scam.

Preventive measures

- Keep your computers and mobile devices up to date
- Set strong passwords
- Watch out for phishing scams
- Keep personal information personal

- ### Cyberstalking

  This kind of Cybersecurity involves online harassment were stalkers use social media, websites and search engines to intimidate a user and instill fear. Usually the cyber stalker knows their victim and makes the person feel afraid or concerned for their safety.



"Hacker X"

tampering and stalking ex-girlfriend online

stealing identities and altering passwords

Threatening her with physical harm

20 year sentence in jail

Preventive measure

- Limit personal information online
- Reset your password frequently

Ransomware

Generally, it Is the most unique because in order for an attack to be successful, it requires a victim to become a willing accomplice after the fact. It locks victim's access to their own data and deletes the same if Ransom is not paid.

Preventive measures

- Set up a firewall
- Conduct cyber awareness program
- Enforce strong password security
- Take periodic backups
- Improve your email security

Password Attack

This is another form of Cybersecurity it can be done ethically or criminally, attackers are. facilitated to use software's that expedites cracking and guessing passwords for their needs.

The best way to prevent password attacks is to adopt best practices for password hygiene and management.

- Requiring long, complex password that are unique for each website or account.
- Adopting a password manager to simplify password management.
- Never leave a default password
- Never use a password that can be found in the dictionary
- Never use a password related to your hobbies, pets, relatives or date of birth.

- Mobile money fraud

  Describes a financial transaction that are conducted using a mobile phone, were a value is stored virtually in an account associated with a sim card. Such transactions are compatible with basic phones and do not require internet connection.

MTN
KAZANG
atlasmara
tilt.
TENGAL
ZOONA
LET'S MAKE IT REAL
Mukuru
Investrust Bank
Afrivance
BARCLAYS

Preventive measures

- never share your pin
- Review your account
- Check your credit report
- Use online transaction with caution

Impacts of Cybercrimes on Businesses

As the use of the internet and networked computers grow, new technologies such as cloud computing enable even greater technology advances. The occurrence of Cybercrimes is expected to grow as cybercriminals seek to exploit online and networked vulnerabilities in business networks. Cybercrime costs the global economy about $445 billion every year, with the damage to business from theft of intellectual property exceeding the $160 billion loss to individuals.

For further understanding

Increased costs

Companies that want to protect themselves from online thieves have to pull out their wallets to do so. This may include;

- Insurance Schemes
- Public relations support
- Cybersecurity technology

Reputation Damage

Trust is an essential element of a customer relationship. Cyber-attacks can damage a business reputation and erode the trust your customers have for you. This could potentially lead to

- Loss of customers
- Loss of sales
- Reduction in profits

Lost Revenue;

One of the worst outcome of a Cyberattack is a sudden drop in revenue. Companies lose money to hackers who try to extort them.

- Hard to get a figure, because a high percentage of Cybercrimes go unreported.

The bottom line

Protecting a business against cyberattacks is costly and can impact the relationship between the company and its customers. As Cybercrime become more sophisticated, businesses will have to stay one step ahead.

Impact of Cybercrimes in Society

- A shield of anonymity
  Due to a large number of connected people and devices today, Cybercrime is a bigger risk now than ever before. The internet, in particular allows offenders to hide behind a shield of digital anonymity making it a great tool for scammers and hackers.

Trending Story

Richard Sakala says he lost k200 in a mobile money scam.

"He concluded that the thieves are just using psychology, because they know that at one point or another someone might be sending money," he says.

It's difficult to change habits when mobile money is so convenient.

"I still use it despite losing such a large amount, says Mulenga the woman who meant to send money to her son. I am just more careful now.

How to tackle Cybercrimes in our society?

The first step to mitigating the threat of cyber-crime within our society is education. Attackers will always target the weakest link in the chain; time and time again, people have been proven to be that weak link. As such, knowledge is power when it comes to tackling cyber-crime.

Recently, there has been a lot of talk about making cyber security a part of the school curriculum, which is a positive step in the right direction. This would help to ensure the next generation is armed with the skills they need to defend against cyber-crimes skills which can then be taken into the workplace. This is particularly important given the current skills gap within the IT security sector.

Furthermore

- Never click on unfamiliar links or ads.
- Use a strong password with different characters
- Become vigilant when browsing websites.
- Keep antivirus/application up to date.

Statistics

In the year 2021 from January to December, the Zambia police at Lusaka division recorded a total number of 86 cases of mobile money fraud with the total amount of money amounting to k726,375 Out of 86 were cases of impersonation and 2 were cases of obtaining money on false pretense amounting to k7,550. The majority of the cases reported were mobile money fraud, as if it's not enough Zambian Cyber Security Initiative Foundation has received a report of 3 Cyber cases and 3 cases of Sextortion.

In conclusion,

The primary step, therefore is to be more aware of the technological advancements and the internet scams that come with it. Taking necessary precautions, securing data entry details and login credentials are of utmost importance as far as staying secure in the digital world.

At Zambian Cyber Security Initiative Foundation, our mission is to promote digital citizenship in this increasingly digital world.

Contact or report the crime at https://www.zcsi-foundation.org/file-complaint/ or you can call us on (+260777680138) or send our office a message to tell us what is going on. We will be in touch right away.

https://www.facebook.com/ZCSIF?_rdc=1&_rdr

https://www.youtube.com/channel/UCN9B1Z5547XolTynxpj9R0w

https://twitter.com/CyberZambia

ZAMBIAN. CYBER. SECURITY. INITIATIVE. FOUNDATION.
ZCSIF

AFRICA CYBERSECURITY
ALLIANCE