VOL
1
2021

DIGITAL SECURITY MEMOIR'S

ZCSIF

Zambian Cyber Security Initiative Foundation is a Zambian owned Local Non-Government Organization. We are into digital security awareness, research, consultancy, training and counseling. We believe in the human factor as the last line of defense in digital security hence our interest in equipping this critical party in the digital ecosystem with defensive information for safe surfing.

VISION

TO HELP IN THE FIGHT AGAINST CYBERCRIME THROUGH AWARENESS AND COLLABORATING WITH RELEVANT LAW ENFORCEMENT AGENCIES IN PROVIDING TRAINING, RESEARCH,TOOLS AND ADVICE AND OUR MISSION STATEMENT BEING PROMOTING DIGITAL CITIZENSHIP IN THIS INCREASINGLY, DIGITAL WORLD.

Our Strategy identifies four cross-cutting principles;

1. "One Team, One Fight"
2. Employment of risk management methodology through awareness and sensitization campaigns
3. Prioritized planning and resourcing
4. Enterprise-wide collaboration

Basic Cyber Security Dictionary:

Encryption: A process of converting the original representation of information, known as plaintext, into an alternative form known as ciphertext. Only authorized parties can decipher a ciphertext back to plaintext and access the original information.

Decryption: A process that transforms encrypted information into its original format with the use of algorithms.

Cyber Space: refers to an environment where the entities and objects that exist within the global computer network (internet) interact

Cyber Attacks: any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices.

Hacker: a computer expert who uses their technical knowledge to achieve a goal or overcome an obstacle, within a computerized system by non-standard means.

Malware: any software intentionally designed to cause damage to a computer, server, client, or computer network. By contrast, software that causes unintentional harm due to some deficiency is typically described as a software bug.

Virus: a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code.

Trojan horse: A type of malware that disguises itself within legitimate applications and software.

Spyware: software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Ransom ware: a type of malicious software designed to block access to a computer system until a sum of money is paid.

What is Digital Security?

Digital security is the collective term that describes the resources employed to protect your online identity, data, and other assets. These tools include web services, antivirus software, smartphone SIM cards, biometrics, and secured personal devices**.** In other words, digital security is the process used to protect your online identity.

What is Cyber Security?

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cyber security measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

Why cyber security?

According to a widely accepted estimate, cybercrime costs the world economy the sum of US $ 500 billion, more than the GDP of South Africa (350.6 billion dollars) and slightly less than that of Nigeria (521.8 billion dollars), the continent's largest economy.

According to the United Nations, cybercrime covers any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Who needs cyber security?

From social media to online banking to digital hospital records, every piece of our lives is available on the internet. Hackers and other nefarious characters can fight to gain access to this information and use it for their own purposes. In essence, everyone needs cyber security. Because just about everyone has personal information available via the internet.

How to Protect:

1. **Online accounts**

   Two-factor authentication, or 2FA, is one of the easiest and most available **multi-factor authentication approaches to protecting online accounts**. Analysis of recent online account breaches indicate that weak and reused passwords continue to be a common entry point for account or identity takeover and network intrusions

2. **Financial information**

   To protect your personal financial information online, use **long and unique passwords**. You can also use pass-phrases instead of passwords because they are more complex to decipher. You should also use two-factor authentication wherever it is available for added security

3. **Emails**

   A strong and separate password for your email account is a good way to help prevent **cyber-attacks** and **protect** your online identity. Have a strong and separate email password.

4. **Networks**

   Encrypt what needs encrypting.

   The problem with data encryption is that it's almost always seen as being a step too far — far too complex, far too expensive, far too much. The truth is that you're usually better off encrypting only the data that is most valuable to your organization. Data that is encrypted strongly enough will be beyond the abilities of most hackers.

   Authentication.

   Authentication refers to the use of password managers and multifactor authentication. Strong passwords should be a no-brainer. But when you throw multiple secure passwords it can be difficult to manage. This is where enterprise, business-grade password managers come in to play.

   Encrypt your most valuable data

   At the very least encrypt your data then use secure deletion tools, such as eraser, on individual files and folders. It overwrites drive space with a series of 35 random patterns.

5. **Mobile Devices**

   Keeping software up to date ensures the best protection against most mobile security threats. Choose mobile security. Just like computers, your mobile devices also need internet security. Make sure to select mobile security software from a trusted provider and keep it up to date. Install a firewall.

What to avoid?

1) **Clicking Random Links:**
   Phishing is the term for sending emails (considered the bait) with a link to a fake website. Once on the site, the user is tricked into giving sensitive information. For example, the link takes you to a fake site that looks like your bank, and you try to log in with your username and password. The bad guy has now captured your login info. And if he's clever then it would redirect you to the real site afterward.
2) **Downloading Counterfeit Software Products:**
   Traditionally counterfeit software often contains malware. A link to a software download site may itself just be a front for a malware download. Activation keys supplied with downloadable product are often are expired, blocked, fake or stolen activation codes. If the keys are invalid your product may not work at all, or will work with reduced functionality, or you may not receive online updates that normally help keep you secure.
3) **Downloading Anonymous Attachments In Email:**
   To avoid infecting your system, please remember to never read or open attachments in emails where you do not recognize the sender, and/or are not expecting an attachment from the sender.
4) **Accessing Suspicious Websites**
   A malicious website is a site that attempts to install malware (a general term for anything that will disrupt computer operation, gather your personal information or, in a worst-case scenario, gain total access to your machine) onto your device.

Steps to Take If:

I. **You have fallen victim to cyber attacks**
If you're a victim of a crimeware attack you should disconnect from the Internet immediately. If you're connected via Wi-Fi, phone or Ethernet cable, you need to disable the connection as soon as possible to prevent data being transmitted to the criminal. Breaking your network connection is the best way to put an immediate stop to the attack.

II. **Your computer system has been infected by a virus**
Start your computer in safe mode and run an anti-virus scan of your entire computer**.** Refer to your computer software supplier's customer support team to see if they offer any tools or resources to extract the virus from your computer. Be sure to delete all of your temporary files in safe mode.

III. **You receive a link for a free shopping voucher you are not expecting**
If you receive an email or text message out of the blue, or come across a social media post, claiming that you can receive a free or heavily discounted voucher, contact the retailer directly to verify the legitimacy of the offer. Don't rely on numbers, email addresses or websites provided.

IV. **You have used the same password for more than 3 months**
Your password is one of the most basic tools you have to keep other people's paws off your data, but the longer you have it, the higher the odds are that cyber criminals will figure it out and abuse it.

V. **Your email has been compromised**
Contact the people in your email address book and let them know that your email was compromised. Remind them to delete any emails from you during the time your account was compromised to prevent them from becoming the next victim. Verify if there is private or personally identifiable information in your e-mail that could be used maliciously.

Internet users are currently growing at an annual rate of 5.7 percent, equating to an average of more than 700,000 new users each day. However, the coronavirus pandemic has had a big impact on internet user research, so actual figures may be much higher.

Most internet users (92.1 percent) use mobile devices to go online at least some of the time, but computers also account for an important share of internet activity.

4.80 billion People around the world use the internet in July 2021 that's almost 61 percent of the world's total population.
This number is still growing too, with our latest data showing that 257 million new users came online over the past twelve months.

APPRECIATION

After a king drive down the digital path coupled with a hype of digital obstacles and hurdles, our feet have brought us to this point with a touch of excellence to our partners who have been with us since the day we started walking.

Special appreciation goes to Zambian National Broadcasting Corporation our all-weather media partner who has not wavered in giving us the visibility we needed while serving the masses of Zambia and all viewers of ZNBC on DSTV.

More appreciations go to Zambia Information Communications and Technology Authority (ZICTA), The Ministry of Community Development and Social Security (MCDSS) and the ICT Association of Zambia for having been so supportive of this noble marathon we took from the onset.

Lastly, we are concluding our appreciation with DefendDefenders our GIF regional partner. Against all odds, this partnership's results will go down in history.

@ZCSIF2019

https://www.zcsi-foundation.org

info@zcsi-foundation.org

THE FUTURE IS HYPERCONNECTED AND CYBER-PHYSICAL AS THE WORLD GOES DIGITAL, THE RAPID PROLIFERATION OF REVOLUTIONARY TECHNOLOGY IS UNLEASHING DANGEROUS NEW CYBER THREATS THAT ARE PUTTING MANY BUSINESSES, CRITICAL INFRASTRUCTURE, EVEN HUMAN LIVES AT RISK. DANGEROUS MALWARE IN ALL ITS FORMS HAS PROLIFERATED IN REACH AND SOPHISTICATION TO EXERT A DEVASTATING TOLL ON SOME ORGANIZATIONS – WITH RANSOMWARE CURRENTLY DOMINATING HEADLINES AMID MASSIVE EXTORTION ATTACKS.

WHILE THE RAPID SHIFT TO ONLINE SERVICES AND REMOTE WORK DURING THE GLOBAL PANDEMIC CREATES NEW OPPORTUNITIES TO LAUNCH LUCRATIVE RANSOMWARE ATTACKS, THE THREAT TO OPERATIONAL TECHNOLOGY-CONTROLLED ENVIRONMENTS HAS BECOME A CRITICAL CONCERN. THE RACE IS NOW ON TO RESPOND WITH SECURITY AND THREAT-MANAGEMENT SYSTEMS THAT CAN EFFECTIVELY COMBAT THE DIGITAL MENACE OF MALWARE AND ULTIMATELY STEM THE TIDE OF DISRUPTION.

SECURING THE HYPERCONNECTED WORLD, AIMS TO OFFER TIMELY INSIGHTS AND GUIDANCE ON HOW TO PREPARE AND RESPOND STRATEGICALLY TO THE FORMIDABLE CYBER SECURITY CHALLENGES THAT LIE AHEAD. THE MESSAGE IS CLEAR – THERE IS NO TIME TO LOSE

web.facebook.com/ZCSIF

DEFENDDEFENDERS
East and Horn of Africa Human Rights Defenders Project

THE GREAT CIPHER MIGHTIER THAN THE SWORD