1st Place – Kennedy Muthii

MALWARE: A THREAT WORTH A GLANCE

Malware has become a common name in the technology field in Kenya. Both private and government-owned institutions use technology in their daily office activities. According to a report published by Business Daily late last year, malware attacks accounted for 50 per cent of all reported attacks in Africa. There was also a rise in the number of attacks experienced last year compared to other years. The Communication Authority, together with the Kenya National Bureau of Statistics, stated that there is a lack of intruder detection mechanisms put in place by institutions to protect their networks. COVID-19 gave criminals a golden chance to launch attacks against Kenyan based firms. Hackers used the malware to gather information, steal money, and ask for ransoms, among other gains.

Banking institutions are one of the sectors which has been hit hard by the surge in attacks, experiencing a loss of about 17 billion to criminals in 2016. In 2017, the Kenya Revenue Authority was siphoned close to 4 billion Kenya shillings. This was money paid as tax by hardworking Kenyans that would have been used for development purposes. It was an eye-opening experience for the government to focus on improving cyberspace safety for both public and private entities by drafting and enacting cyber laws. E-commerce and telecommunication companies have not been spared. Through the collaboration of international and local institutions, cyber talent training programmes have been established to prepare cyber professionals to combat cybercrimes.

Hospitals and health providing facilities also had a share of the malware blow. Hackers targeted information collected from the patients. Such information would later be used for identification purposes by the hackers to steal cash or other reasons. Ransomware attacks have also thrived in this sector as the hackers encrypt vital customer and financial data and ask for large sums of cash which has to be paid anonymously. The government advises the institutions not to conform to the hackers' demands as there is no guarantee that they will have encrypted information back. The government has also set yo a cyber team to help public health institutions back on their feet after the attacks.

In the field of politics, there have been reports on cases of hacking. For example, during 2017 there were reports of a failed hacking attempt against election systems. The government had tighter measures put in place since this happened after the Kenya Revenue Authority hack. Hackers use malware delivered through sophisticated techniques to steal social media accounts and login details of influential political figures and use them to spread misleading information to the public. Various avenues are available where the government trains the public on identifying fake news.

Conclusion

With the rise of cybercrime, as a country, we need to train and prepare ourselves to fight at a world-class level. Cybersecurity policies have to be set in small businesses and institutions to ensure the cyber safety of Kenyan citizens as they transact and share information with the institutions. For the country to thrive, both politically and economically, we need to understand cybersecurity taking it as a personal responsibility.

References

https://www.businessdailyafrica.com/bd/news/kra-seeks-cyber-crime-solution-after-sh4bn-theft-2157530
https://www.businessdailyafrica.com/bd/corporate/companies/police-probe-130-bank-cyber-fraud-suspects-2236886
https://www.businessdailyafrica.com/bd/corporate/technology/kenya-reports-highest-cyber-attacks-in-africa-2370444

2nd Place – Evelyne Okado

On 19th June 2021, I found out that I was a member of Amani National Congress Party (ANC). In any other circumstance, this would have been good news, but the circumstances were different. I was registered to a political party without my consent. Well, I wasn't the only one registered. On this very Saturday, most people, especially those who had registered to get a Huduma number, found out that they were registered to political parties they had no affiliation with.

The politics of it all aside, finding ourselves registered illegally to an unfamiliar political party didn't quite shock me or anyone for that matter. It was actually funny because compared to the questionable things our government does every day, illegally sharing our data with other entities was at the bottom of the 'did they really do that' list. We constantly wake up to text messages from subscription services we didn't subscribe to since our telecommunication companies auction our data to the highest bidders. These third parties also have access to our airtime balance and deduct it whenever they see fit. Without even batting an eye, these same telecommunication companies act surprised when we inquire how these third parties got access to our phone numbers.

Kenya is no stranger to political tension. In fact, the country never takes a break from politics. There have been claims that elections have been stolen before. Some polling stations have previously submitted election results indicating that the total votes cast were higher than the number of registered voters. So, the timing of the incident wasn't helpful. In a country that has experienced post-election violence, sharing such sensitive data with third parties only sparks suspicion and political tension. Political tension only breeds hate and contempt and slowly leads the country into a tense election period.

In the case involving the registrar of political parties and the various telecommunication companies, we had no control of what would be done with our data. However, it's our collective responsibility to be cautious with who we share our data with. It's also upon us to demand accountability from these entities and ensure that they are compliant with the set data regulations.

The Kenyan Personal Data Protection Act

In 2019, Kenya passed the Kenya Personal Data Protection Act to protect personal data. It was seen as a significant step to facilitate the lawful use of data and protect individual rights. The law regulates the use, processing, and storage of personal data. It also established the Office of the Data Protection Commissioner to make provisions for regulating the processing of personal data, specify the roles of the data processors and controllers, and stipulate the data subjects’ rights.

The data protection act requires that all personal data be processed lawfully and transparently concerning the subject. The act provides that the data subject has a right:

- To know what use their data is to be put
- Have access to their data
- To object to the processing of some or all of their data
- Correct false and misleading data out themselves
- Delete false and misleading data about themselves

While the act has been passed, it remains just that — laws. The Kenya Personal Data Protection Act was mainly passed to comply with the European Union Data Protection Act. While this has opened up the country to numerous investors, implementation of the act has proved challenging. Two years after the bill was passed in parliament, the people we entrust our data with don’t provide any transparency in how our data is handled.

3rd Place – Kennedy Nyakoe

This essay is about the importance of why cybersecurity is a shared responsibility among Kenyan citizens and the importance of it.

Cybersecurity refers to how we secure and protect our internet-connected systems through established technologies, processes, and controls from cyber-attacks.

With millions of Kenyans living on the internet, most of the users are generally ignorant on how to stay safe online. Whether requesting a cab or booking a hotel they are constantly generating lots of data and this data is stored online in form of cloud data in data centers. For a hacker in this digital era, it's a gold mine with tons of access points, public IP addresses, and constant traffic. Hackers are having a field day exploiting vulnerabilities and systems. Hackers are becoming smarter each day and by them being able to bypass the security controls it is baffling.

It is a collaborative objective in the sense that, picture a scenario where one computer system is compromised, it can lead to lots of compromised accounts. Imagine a scenario with many? There is a need to implement best practices and policies regarding cyber security. It's a collective initiative and not only a role for the people in the IT industry, as people think.

Whether personal or professional, there is a need for Kenyan citizens to protect their data. This means Kenyan individuals should not go about inputting their data carelessly. For the professional aspect, it's important to protect your organization's critical data assets from risky security risks. There is a need for Kenyan citizens to be educated on cyber security best practices and instill a culture of cybersecurity awareness in them. Kenyans are highly gullible to maldvertisement which ends up duping them to input their personal information that puts them at risk. For example, during the Covid-19 period, Kenya and the Department of Homeland Security warned about scams related to Covid-19. Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19 related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

There are some good cyber security practices that Kenyans need to emulate such as:

- Good password management practices;
- Good knowledge of phishing schemes and scenarios;
- How to do data backup;
- Use and sharing of personal data.

The Kenyan government is involved and has taken a role by enacting the Computer Misuse and Cybercrimes Act of 2018 that aims at protecting the confidentiality, integrity, and availability of computer systems, programs, and data as well as facilitate the prevention, detection, investigation, and punishment of cybercrimes.