Chioma
Ekwelundu

Cybersecurity & Data Privacy

Women as Digital Defenders

IWD2025

Chioma Ekwelundu is a trailblazing cybersecurity advocate, AI-driven digital awareness educator, and multilingual professional committed to empowering women to become digital defenders in today's evolving cyber landscape. A Cohort 2 Fellow at 3MTT, she has actively contributed to cybersecurity education, simplifying complex cyberthreats and data privacy concepts to help individuals and businesses stay secure online.

Chioma holds a degree in French from Nnamdi Azikiwe University, Awka, which has sharpened her communication skills and ability to bridge the gap between technical knowledge and real-world application. She is also certified in cybersecurity by 3MTT, alongside Career Essentials in Cybersecurity by Microsoft & LinkedIn, AI Career Essentials (AICE) by ALX, and HSSE Levels 1, 2, and 3. Through engaging awareness campaigns, she has helped small business owners, professionals, and everyday internet users identify cyber risks and implement proactive security measures.

Beyond cybersecurity, Chioma is a certified makeup artist with an eye for beauty and detail. She also runs a successful online jewelry and footwear store, applying her expertise in digital security to protect transactions and customer data—proving that cybersecurity is essential for entrepreneurs, not just tech professionals.

As a speaker at Women as Digital Defenders – International Women's Day 2025, Chioma is on a mission to equip women with the skills and confidence to take charge of their digital safety, advocating for a safer, more inclusive online space.

WHAT ARE CYBERTHREATS?

Cyberthreats refer to any malicious activity or event that seeks to compromise the security of a computer system, network, or digital device. These threats can manifest in various forms, ranging from malware infections to sophisticated social engineering attacks. Cyberthreats are designed to exploit vulnerabilities in technology or human behavior to steal, disrupt, or manipulate information.

TYPES OF CYBERTHREATS

Internal and External Threats

Cyberthreats can be categorized into two primary types: internal and external threats.

A. Internal Threats:

These originate from within an organization, typically involving employees, contractors, or other trusted insiders. Internal threats can be accidental or intentional. For instance, a disgruntled employee might intentionally leak sensitive data, or an employee might accidentally click on a malicious link, leading to a security breach.

Example:

The 2013 data breach at Target was partially attributed to an internal threat when an employee at a third-party vendor was phished, leading to the theft of credentials that granted access to Target’s network. This breach exposed the credit card information of millions of customers.

TYPES OF CYBERTHREATS

Internal and External Threats

B. External Threats:

These originate from outside the organization and are typically carried out by cybercriminals, hackers, or even state-sponsored actors. External threats can involve
sophisticated attacks aimed at gaining unauthorized access to an organization's systems or data.

Example:

The 2021 SolarWinds attack is a prime example of an external threat, where suspected
state-sponsored hackers infiltrated the systems of multiple U.S. government agencies
and private organizations through a software supply chain attack.

Examples of external threats:

1. **Malware**:

Malware is a general term for malicious software designed to disrupt, damage, or gain
unauthorized access to systems.

Example:

The WannaCry ransomware, a type of malware, affected over 200,000 computers in
2017 by encrypting files and demanding ransom payments.

2. **Virus**:

A type of malware that attaches itself to a legitimate program or file, spreading from
one computer to another as users share infected files.

Example:

The ILOVEYOU virus, which spread through email attachments in 2000, caused billions of dollars in damage globally

Examples of external threats:

3. Social Engineering:

Manipulating individuals into divulging confidential information through deceptive means, exploiting human psychology rather than technical vulnerabilities.

Example:

The 2013 Twitter hack, where attackers used social engineering to gain access to highprofile accounts and post unauthorized tweets.

4. **Phishing**:

A technique where attackers impersonate legitimate entities to trick individuals into
providing sensitive information.

Example:

The 2016 phishing attack on the Democratic National Committee (DNC) led to a significant data breach and public exposure of private emails.

How To Protect Ourselves / Preventive Measures

Authentication: Update your passwords, face IDs, Fingerprints. Every device without authentication is at RISK of attacks. Face ID is one of the biggest security now(external threats) also Google authentication is highly recommended because it's hard to hack.

Authorization : PII/SPII is necessary in Authorization, that's Personal Identifiable Information/ Secret Personal Identifiable Information. This is what distinguishes you. Examples of SPII in Nigeria is NIN and BVN.

Conclusion:

Cyberthreats are diverse and evolving, with both internal and external sources posing
significant risks to individuals, businesses, and governments. Understanding thes threats, from malware and phishing to more advanced social engineering techniques,
is essential for developing effective cybersecurity strategies. By being aware of these
risks and implementing proactive measures, organizations can better protect themselves from potential cyber incidents.

Chioma
Ekwelundu

THANK TOU

For watching this presentation

Chioma Ekwelundu

+2347039738255

chiomaekwelundu@gmail.com

Pot Harcourt, Rivers State,
Nigeria