USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

CTO PEER MENTORING PROGRAM

TOPIC 2 MENTOR SESSION

INTRODUCTION

This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Establishing and Implementing a Cybersecurity Employee Training Program & Testing Program

WHAT IS CYBERSECURITY EMPLOYEE TRAINING?
ALSO KNOWN AS CYBERSECURITY AWARENESS TRAINING

Cybercriminals take advantage of users' trust, fear, greed, and plain old human errors.

Security awareness training teaches users to spot phishing, avoid risks online, and use good cyber-hygiene practices at work and at home.

Users constitute the theory of a "bio-sensor", which is the concept of employees/users representing a distributed detection capability.

WHY DOES TRAINING MATTER?

- The world is becoming more digital
  - Business, banking, healthcare and so on is all online
- Crime is following the same trend
  - Worldwide ransomware attacks
  - High-profile hacks in the news
  - Phishing emails are more sophisticated each day
- New privacy laws and regulations are being enacted
  - Many sectors require training for compliance
- Globalization
  - Globalization facilitates actions on objectives at scale
  - Denial of service for ransom, denial of data for ransom, reputation for ransom…

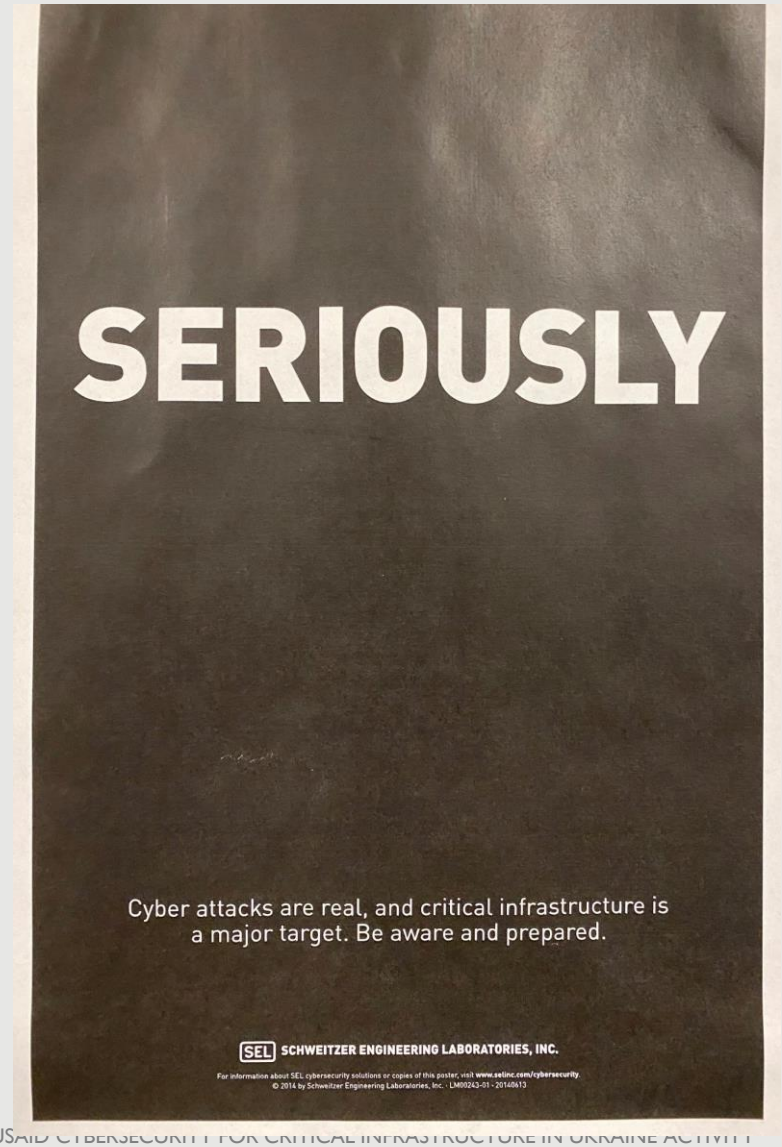
WHY SHOULD USERS CARE?

- Because the online world is so interconnected, everyone is a target of opportunity
- If just one of your accounts gets breached, criminals can use it to breach others
- Criminals may target personal accounts and data to breach corporate ones, and vice versa
- Fraud and identity theft don't just affect an individual; it can affect user accounts belonging your family, friends, coworkers, and business

WHAT KIND OF THREATS ARE THERE?

- Phishing and spear-phishing attacks
- Business email compromise
- Social engineering scams
- Common malware and ransomware
- Fake websites that steal data or infect devices
- And much more

HOW TO GET STARTED…



HOW DOES SECURITY AWARENESS TRAINING HELP INDIVIDUALS AND ORGANIZATIONS?

- Prevent intrusion in a business infrastructure
- Reduce business email compromise
- Keep critical business data safe
- Protect your identity and personal data from theft and fraud
- Secure your devices against viruses and malware
- Keeps you safe from hackers and spies

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

QUESTIONS AND ANSWERS