USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПРОГРАМА НАСТАВНИЦТВА ДЛЯ ТЕХНІЧНИХ ДИРЕКТОРІВ

Тема 2. Вступ

Ця презентація була підготовлена на замовлення USAID. Її самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цій презентації, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Розробка та реалізація програми підготовки співробітників у сфері кібербезпеки

ЩО ЯВЛЯЄ СОБОЮ ПІДГОТОВКА СПІВРОБІТНИКІВ У СФЕРІ КІБЕРБЕЗПЕКИ?

- Також відома як підвищення обізнаності співробітників у сфері кібербезпеки
- Кіберзлочинці користуються довірою, страхами або типовими людськими помилками користувачів
- Підвищення обізнаності у сфері заходів безпеки навчає виявляти фішинг, уникати ризиків в мережі Інтернет та дотримуватись норм кібер-гігієни вдома або на роботі
- Користувачі долучаються до теорії «біодатчиків», що приймає співробітників / користувачів за розгалужену систему виявлення

В ЧОМУ ВАЖЛИВІСТЬ ПІДГОТОВКИ?

- Роль цифрових технологій у світі зростає
  - Підприємницька, банківська, медична та інші сфери діяльності переходять в режим онлайн

- Аналогічна тенденція спостерігається серед злочинності
  - Атаки з використанням програм-вимагачів в усіх країнах світу
  - Інформація про резонансні хакерські атаки в новинах
  - Продуманість електронних листів для фішингу зростає з кожним днем

- Запровадження нових законів та нормативних актів у сфері конфіденційності
  - Чимало секторів потребують проведення підготовки у сфері дотримання вимог законодавства

- Глобалізація
  - Глобалізація збільшує масштаби вчинення шкідливих дій у геометричній прогресії
  - Відмова в обслуговуванні до отримання викупу, відмова в доступі до даних до отримання викупу, захист репутації в обмін на викуп…

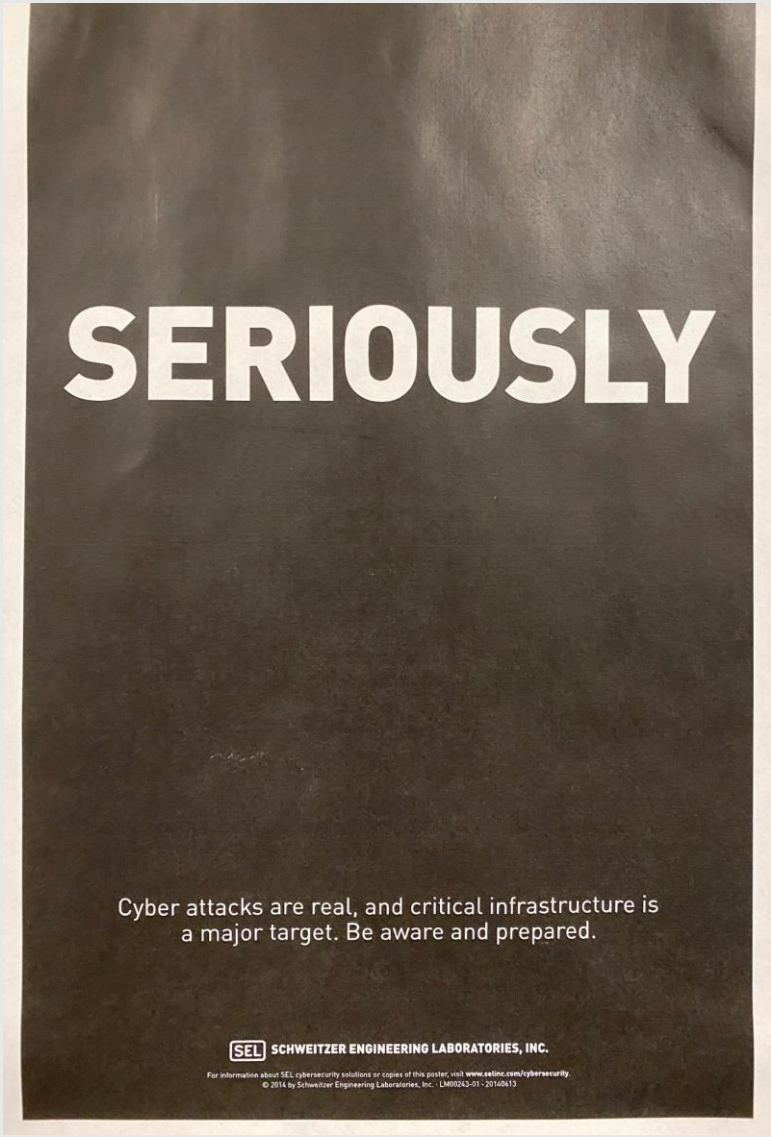
ЧОМУ ЦЕ ВАЖЛИВО ДЛЯ КОРИСТУВАЧІВ?

- У віртуальному світі всі взаємопов'язані, а тому кожен може перетворитись на мішень для нападу
- Отримавши доступ до одного облікового запису, зловмисники можуть скористатись ним для отримання доступу до інших
- Зловмисники можуть націлюватись на особистий обліковий запис або дані з метою отримання доступу до корпоративного і навпаки
- Шахрайські дії або викрадення особистості можуть зачепити не лише одну особу – вони можуть вплинути на облікові записи користувачів, що належать вашій родині, друзям, колегам або компанії

ЯКІ ТИПИ ЗАГРОЗ ІСНУЮТЬ?

- Фішингові атаки та цільовий фішинг
- Отримання доступу до корпоративної електронної пошти
- Психологічні атаки шахрайського характеру
- Зловмисне програмне забезпечення та програми вимагачі
- Фіктивні веб-сайти для викрадення даних або інфікування пристроїв
- ...

З ЧОГО ПОЧАТИ…



В ЧОМУ КОРИСТЬ ПІДВИЩЕННЯ ОБІЗНАНОСТІ У СФЕРІ БЕЗПЕКИ ДЛЯ ОКРЕМИХ ОСІБ ТА ОРГАНІЗАЦІЙ?

- Профілактика втручання в інфраструктуру бізнесу
- Профілактика несанкціонованого доступу до корпоративної електронної пошти
- Захист особливо важливих комерційних даних
- Захист власної особистості та особистих даних від викрадення або шахрайських дій
- Захист власних пристроїв від вірусів та зловмисного програмного забезпечення
- Захист від діяльності хакерів та шпигунів

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПИТАННЯ ТА ВІДПОВІДІ