Кібербезпека - уроки війни, та практичний вимір

Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики

25 жовтня 2023 р.

vnu.edu.ua

Оксана Жигаревич
Старший викладач кафедри
комп'ютерних наук та кібербезпеки

Володимир Гаращенко
CISO @ SOC Prime

SOC Prime - спеціалізуємося на Кібербезпеці

CONNECTING

30,000+ Users

600+ Threat researchers

8,000+ Organizations

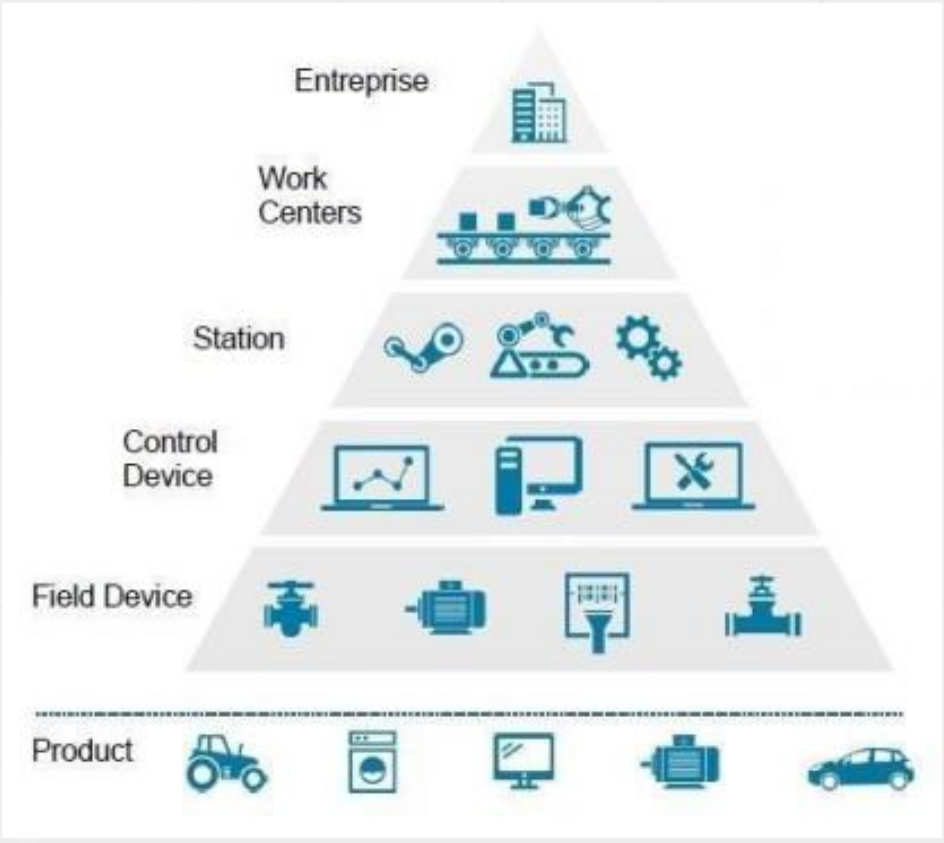
TRUSTED BY

42% Fortune 100

30% Global 500

21% Global 2000

Діджиталізація усюди: Держустанови, ЗВО, підприємства & IoT & OT & Connected cars & Satellite...

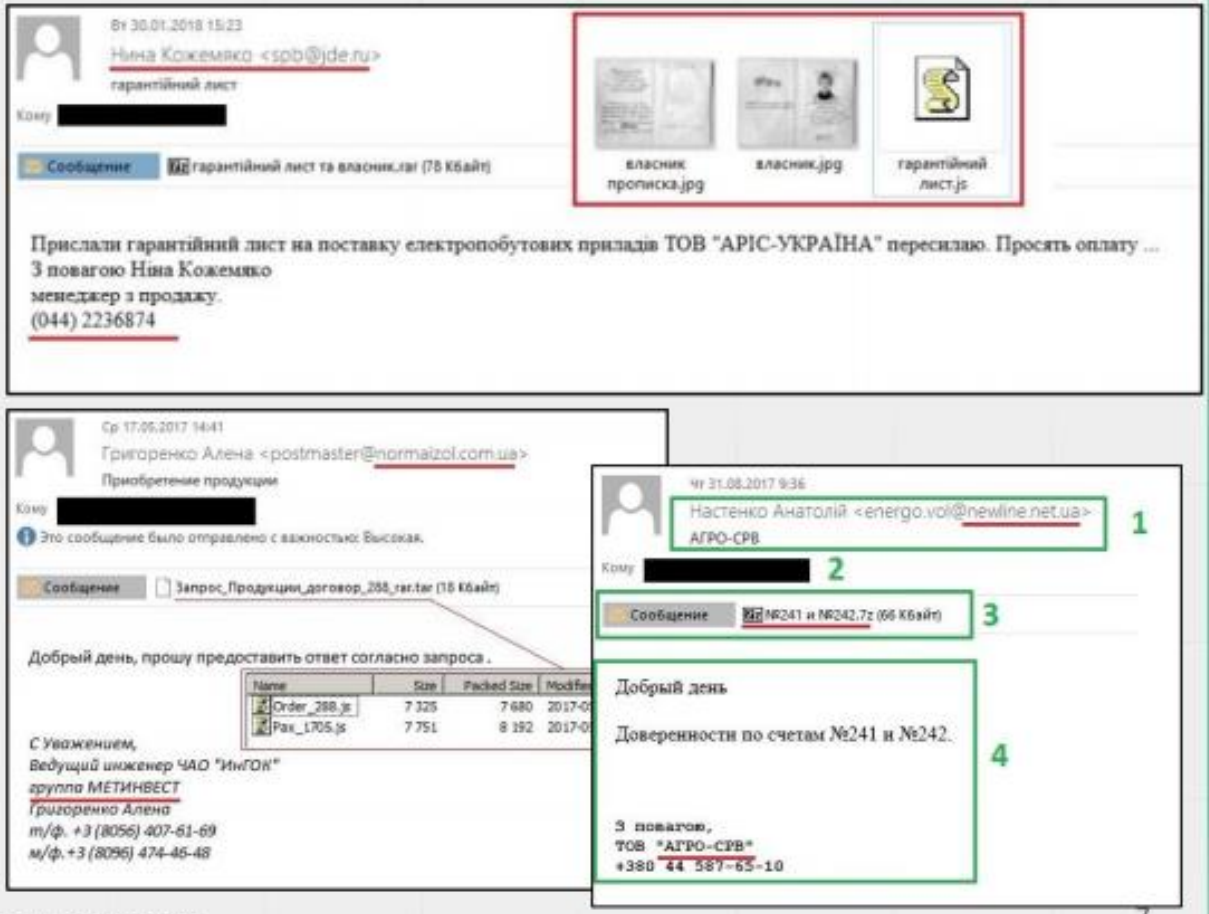


Фішинг - від англ. “Риболовля” на приманку

Фішинг - це підроблені листи або повідомлення в мессенджерах, які нібито надходять від імені банків, державних установ, підрядників, операторів послуг тощо.

Дуже схожі на справжні, інколи навіть гарніші за справжні :)
Мета: змусити Вас щось зробити:

- для крадіжки логіну та паролю – ввести ваші дані на підроблених сайтах, що дуже схожі на справжні.
- для інфікування комп’ютера відкрити або запустити вкладений файл. Word, Excel, PDF, тощо



Базовий захист в соціальних мережах

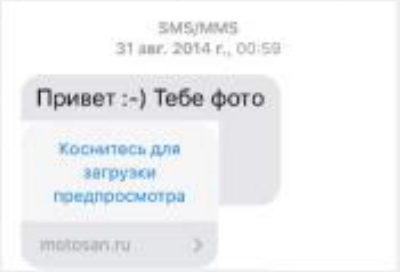
Для безпечного використання соцмереж радимо:
https://cyberpolice.gov.ua/article/pravyla-bezpechnogo-korystuvannya-soczialnymy-merezhamy--porady-kiberpolicziyi-8783/

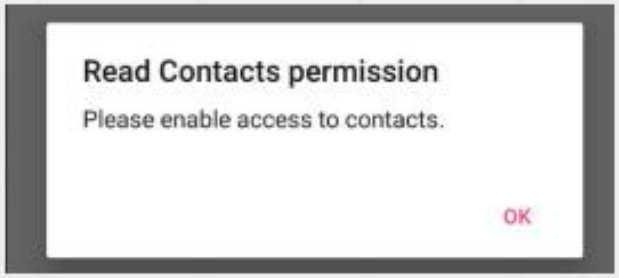
- Обов'язково використовуйте двофакторну аутентифікацію – це найкращий захист для ваших акаунтів, вирішує 90% можливих проблем. **Google Authenticator / Microsoft Authenticator**
- Використовуйте складний пароль, різний для кожної соцмережі!!!
- Не заходьте до своїх акаунтів з чужих пристроїв.
- Ніколи не пересилайте приватні фото або фотокопії документів, у разі зламу ці дані опиняться у зловмисників.
- Не переходьте за сумнівними гіперпосиланнями.

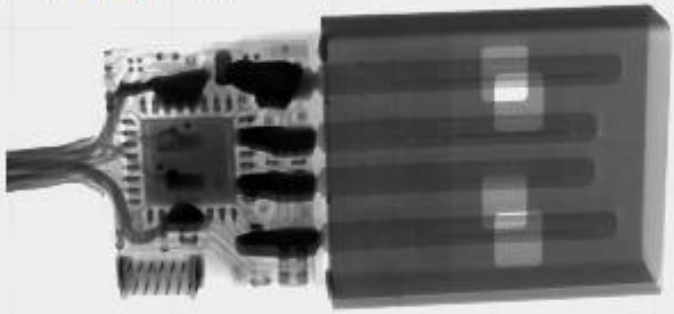
Також варто пам'ятати, що представники соцмережі ніколи не писатимуть в особисті повідомлення, а лише на пошту, вказану при реєстрації.

Базовий захист мобільного телефона

- Здійснюйте регулярне оновлення операційної системи та іншого програмного забезпечення для зменшення кількості вразливостей, через які зловмисники можуть інфікувати пристрої.
- Використовуйте складні та унікальні паролі та пін коди для захисту доступу до телефону.
- Не залишайте розлочений телефон без нагляду.
- Не підключайте смартфон до зарядних дротів у підозрілих місцях.
- Не використовуйте чужі дроти для зарядки телефона від комп'ютера (O.MG CABLE)
- Використовуйте двофакторну аутентифікацію для захисту облікових записів Apple ID та Google, що пов'язані з Вашим телефоном, від несанкціонованого доступу.
- Завантажуйте додатки перевірених розробників. В Інтернеті Ви можете знайти детальну інформацію про розробника чи окремий додаток, відшукати веб-сайт чи контактні дані.
- Читайте про що застерігає Вас телефон, коли Ви відкриваєте посилання чи завантажуєте щось, навіть якщо отримали це посилання на прикольних котиків від друзів.





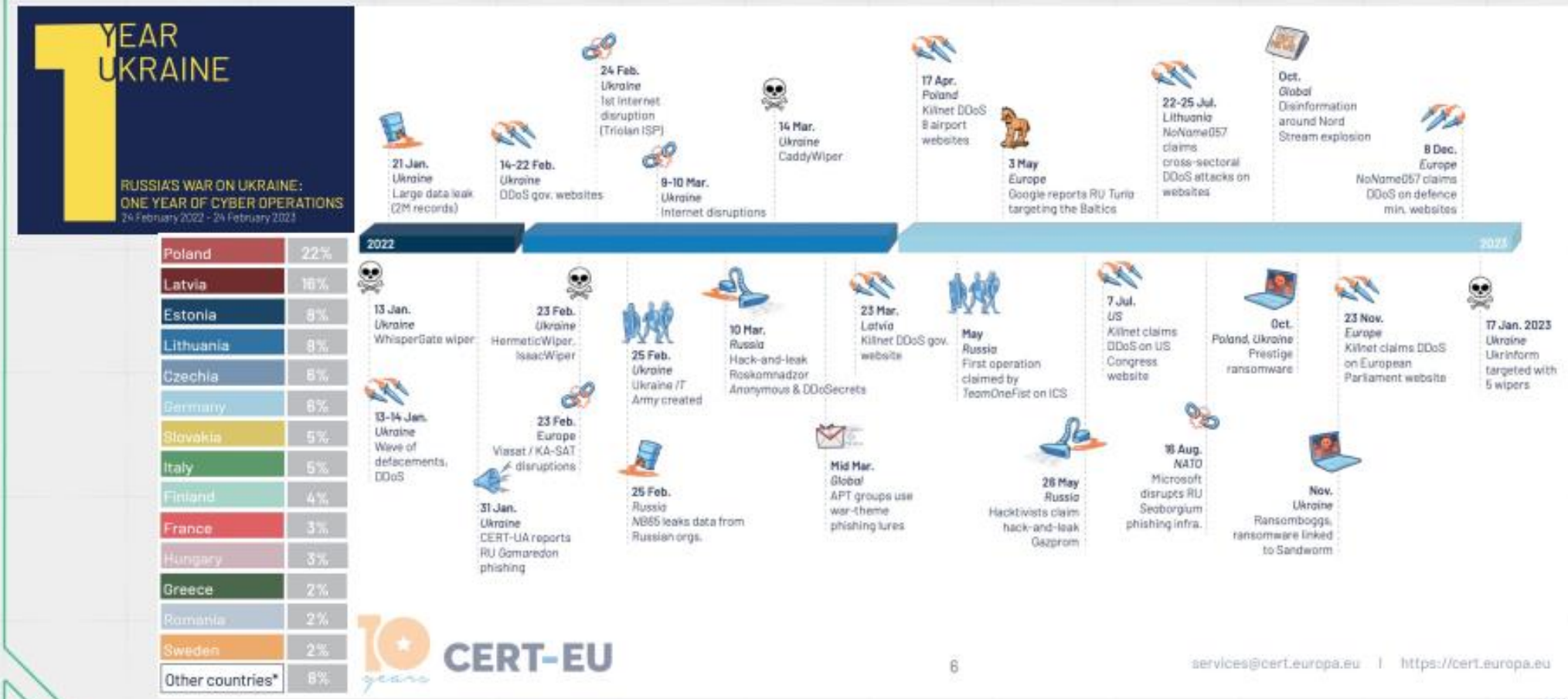


Базовий захист персонального комп'ютера

- Створюйте надійні, складні паролі та не використовуйте однаковий пароль для кількох ресурсів. Пароль має містити не менше 8 символів, літери, цифри та спеціальні символи, а також не містити персональних даних.
- Не використовуйте зламане ПЗ або ПЗ для обходу активації (типу KMS Activator) - безкоштовний сир тільки в мишоловці!
- Обов'язково використовуйте Антивірусне ПЗ, не безкоштовне, не зламане, не китайське…
- Не переходьте за сумнівними гіперпосиланнями, навіть якщо вони надійшли у листі від друга. Пам'ятайте, що хакери могли зламати його акаунти і розсилати з них посилання, за якими ховається вірус або фішинговий ресурс.
- Перевіряйте правильність URL-адреси необхідного сайту. Будь-які неточності можуть означати, що ви потрапили на фішинговий ресурс.
- Регулярно створюйте резервні копії. Це врятує від втрати важливої інформації.
- Завантажуйте програми та додатки лише з офіційних джерел.
- Вчасно встановлюйте оновлення операційної системи та програм.

Windows Defender

CERT-EU: Війна росії проти України. Рік кібер-операцій.



Обізнаний означає попереджений

- Не бійтеся застосовувати свій життєвий досвід у кіберпросторі
- Вивчайте, інформація навколо, можливостей зараз як ніколи багато
- Читаємо актуальні новини на CERT UA (https://cert.gov.ua/articles)
- Долучайтесь до кіберзахисту України, можливостей до кольору до вибору (ну всі ж є в каналі Мрія? https://t.me/stoprussiachannel)

Кожен з нас здатний зробити цей світ трошки безпечнішим.

/Stay Safe