

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 Гарашенко
CISO @ SOC Prime

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

Everyday Things get connected For Smarter Tomorrow

IOT in Agriculture

Embedded System

Smart Retail

Internet of Things

Wireless Connection

Smart Homes & Cities

Vehicle, Asset, Pet Monitoring & Controlling

citycard

HACK ASIN 3
Learn. Space. Faster.

The Car Hacker's Handbook
A Guide for the Penetration Tester



Фішинг - від англ. "Риболовля" на приманку

Фішинг - це підроблені листи або повідомлення в месенджерах, 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

Вт 30.01.2018 15:23
Ніна Кожемяко <sob@jde.ru>
гарантийний лист

Кому [Redacted]

Сообщение [гарантийний лист та власник.jpg](#) (75 Кбайт)

власник прописки.jpg власник.jpg гарантийний лист.js

Прислали гарантийний лист на поставку електропобутових приладів ТОВ "АРИС-УКРАЇНА" пересилаю. Просьба оплату ...
З повагою Ніна Кожемяко
менеджер з продажу.
[\(044\) 2236874](tel:+380442236874)

Ср 17.06.2017 14:41
Тригоренко Алена <postmaster@normaizol.com.ua>
Приобретение продукции

Кому [Redacted]

Сообщение [Запрос_Производства_договор_288.rar.rar](#) (18 Кбайт)

Добрый день, прошу предоставить ответ согласно запроса.

Name	Size	Packed Size	Modified
Order_288.js	7 325	7 680	2017-06-17 14:41
Рак_1705.js	7 751	8 192	2017-06-17 14:41

С Уважением,
Ведущий инженер ЧАО "ИнГОН"
группа МЕТИНВЕСТ
Тригоренко Алена
т/ф. +3 (8056) 407-61-69
м/ф. +3 (8056) 474-46-48

Чт 31.08.2017 9:36
Настенко Анатолий <energo.voi@newline.net.ua>
АГРО-СРВ

Кому [Redacted]

Сообщение [№241 и №242.7z](#) (66 Кбайт)

Добрый день
Доверенности по счетам №241 и №242.

З повагою,
ТОВ "АГРО-СРВ"
[+380 44 587-65-10](tel:+380445876510)

Базовий захист в соціальних мережах

Для безпечного використання соцмереж радимо:

<https://cyberpolice.gov.ua/article/pravyla-bezpechnogo-korystuvannya-soczialnymy-merezhamy--porady-kiberpolicziyi-8783/>

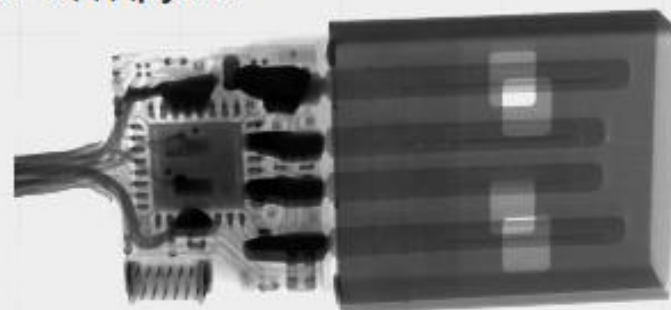
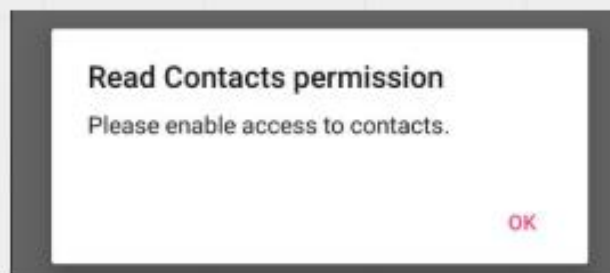
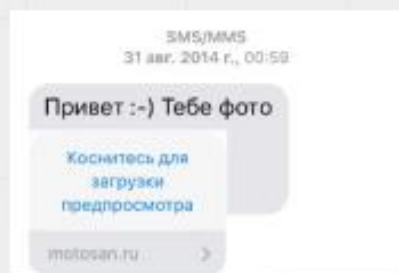
- Обов'язково використовуйте двофакторну аутентифікацію – це найкращий захист для ваших акаунтів, вирішує 90% можливих проблем. **Google Authenticator / Microsoft Authenticator**
- Використовуйте складний пароль, різний для кожної соцмережі!!!
- Не заходьте до своїх акаунтів з чужих пристроїв.
- Ніколи 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 телефону

- 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 телефону 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.



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

1 YEAR UKRAINE

RUSSIA'S WAR ON UKRAINE:
ONE YEAR OF CYBER OPERATIONS
24 February 2022 - 24 February 2023

Poland	22%
Latvia	16%
Estonia	8%
Lithuania	8%
Czechia	8%
Germany	8%
Slovakia	5%
Italy	5%
Finland	4%
France	3%
Hungary	3%
Greece	2%
Romania	2%
Sweden	2%
Other countries*	8%



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

