Правила поведінки при роботі з ІТ.

Владислав Радецький

12 / 05 / 17

Чому я тут ?

Владислав Радецький

Technical Lead, CEH

В IT галузі офіційно з 2007 року.

Починав як адмін / “anykey`щик”.

4 роки працював в IT-аутсорсингу.

З 2011 працюю в компанії БАКОТЕК®

Прийшов сюди щоб поділитися із вами досвідом і знаннями.

https://radetskiy.wordpress.com

http://ua.linkedin.com/pub/vladislav-radetskiy/47/405/809

Головні моменти:

- Людський фактор. Обман. Маніпуляція.
- OSINT, правильна обробка інформації.

Теми, які часто ігнорують
(Бо вони складні в роботі)

- **Приклади свіжих кібератак 2017**
- Практичні рекомендації
  - Паролі
  - Передача інформації
  - Email
  - Додатки, чужі системи, соц. мережі
- Висновки

Безпека держави залежить від вчинків кожного з нас

Трохи прикладів типової людської необережності

Людський фактор

2012 – Фото принца Вільяма розкрили паролі авіабази ВПС Англії

Людський фактор

2014 – Чемпіонат світу з футболу, центр безпеки, пароль Wi-Fi

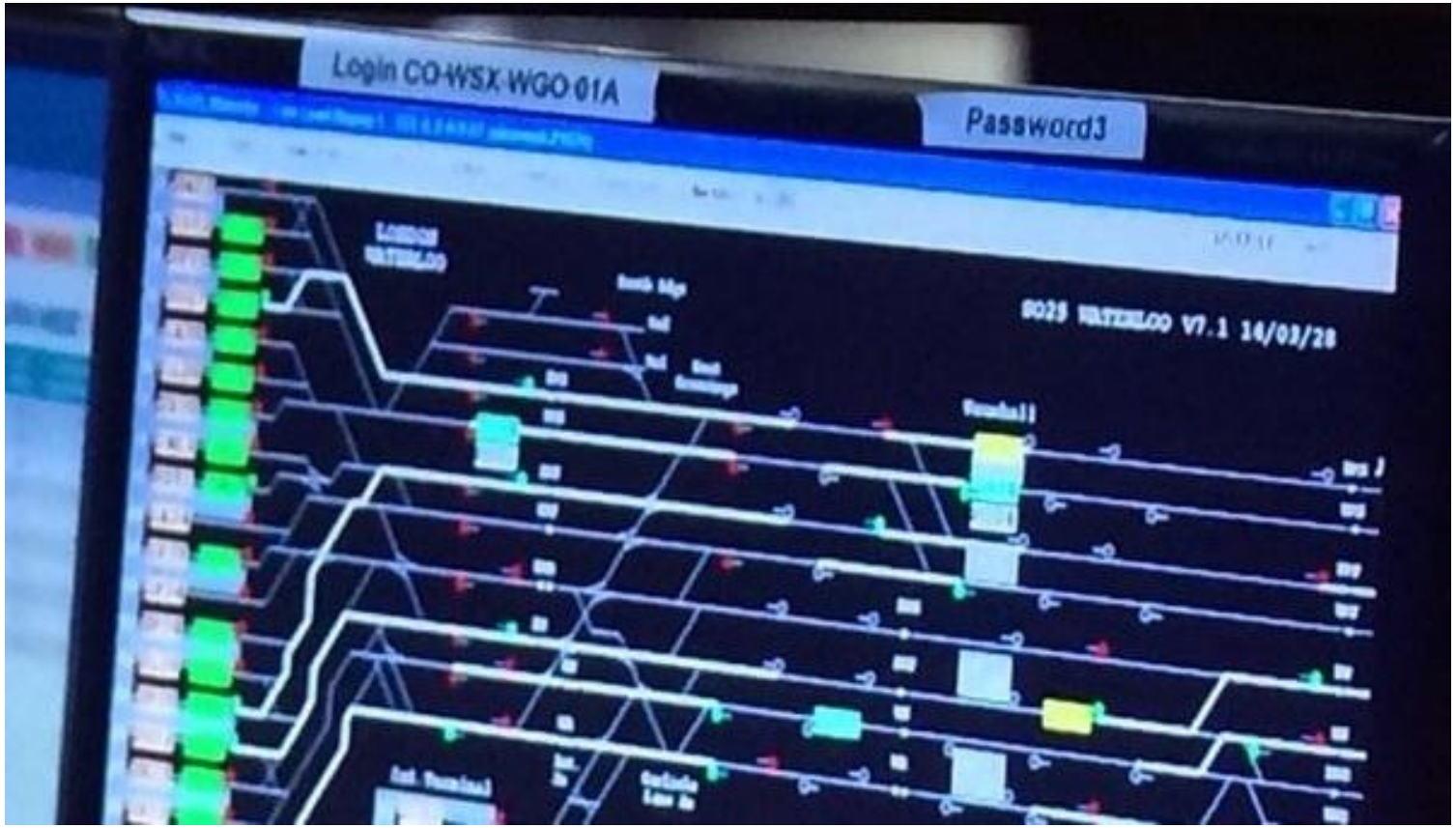
b5a2112014

Людський фактор

2015 – Канал TV5Monde “засвітив” свої паролі під час інтерв'ю

Людський фактор

2015 – В сюжеті BBC “засвітили” паролі залізничної системи Ватерлоо

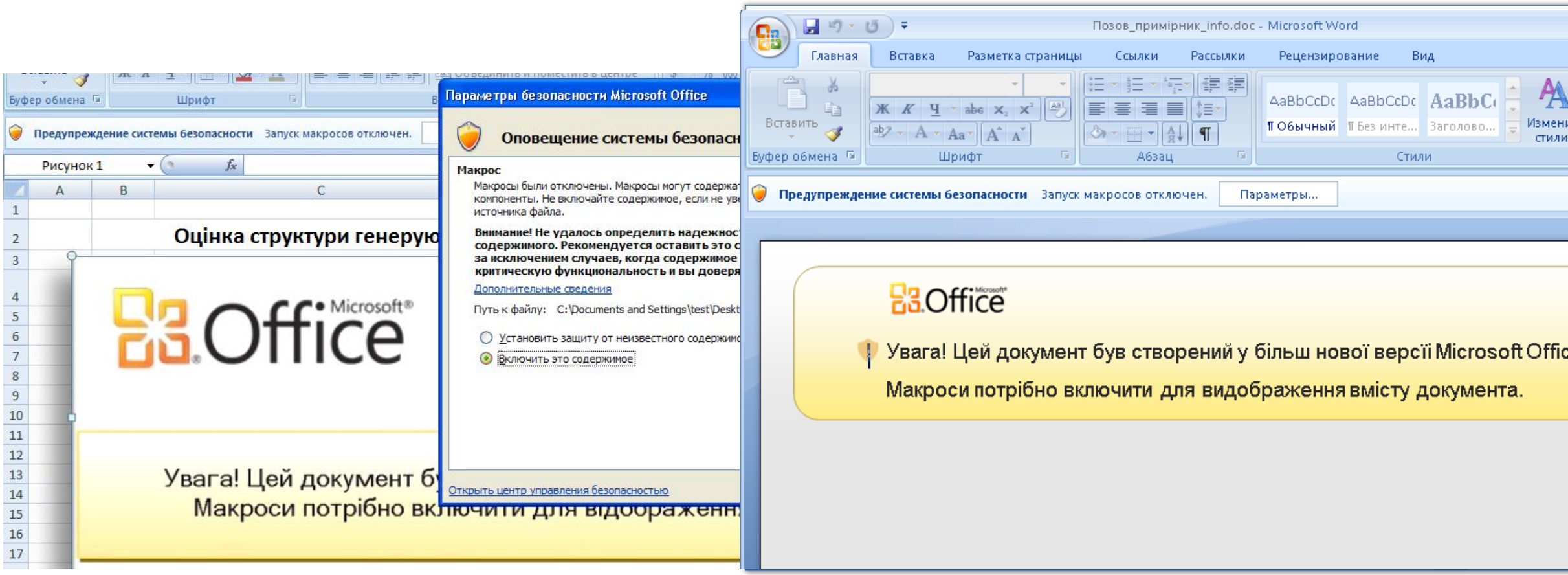


Людський фактор

Ваша черга ?

Людський фактор

2016 / 2017 – люди продовжують клікати “активуйте макроси”



Особливості роботи ПК/гаджетів

Навіть коли система “висне” – в фоні іде купа звернень

- Від обману до шифрування як правило **3-4 кліки**

Особливості роботи ПК/гаджетів

Навіть коли система “висне” – в фоні іде купа звернень

- Від обману до шифрування як правило **3-4 кліки**
- Шифрувальщику треба від **30 секунд** до **15 хвилин**

Особливості роботи ПК/гаджетів

Навіть коли система “висне” – в фоні іде купа звернень

- Від обману до шифрування як правило **3-4 кліки**
- “Шифрувальщику” треба від **30 секунд** до **15 хвилин**
- Ціна помилки стартує від **$ 300**

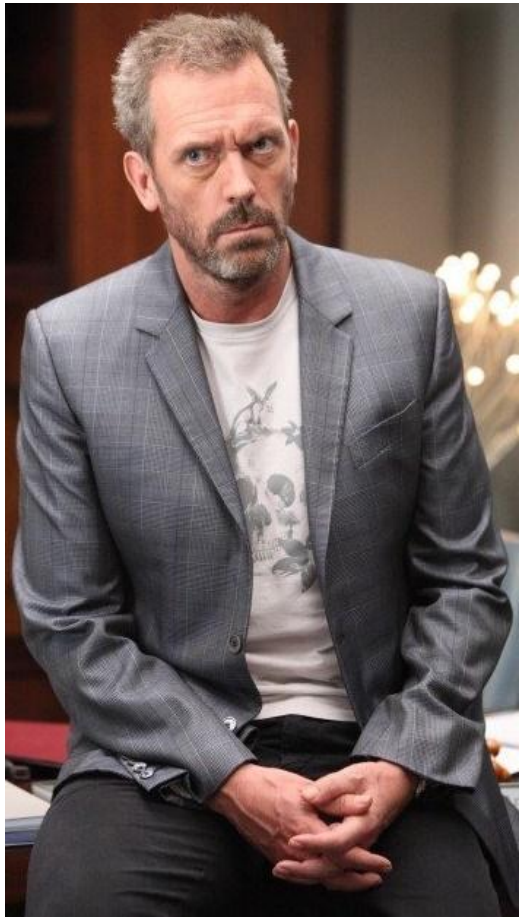
Особливості роботи ПК/гаджетів

Навіть коли система “висне” – в фоні іде купа звернень

- Від обману до шифрування як правило **3-4 кліки**
- “Шифрувальщику” треба від **30 секунд** до **15 хвилин**
- Ціна помилки стартує від **$ 300**
- Більшість жертв не встигають опам'ятатися

Людський фактор

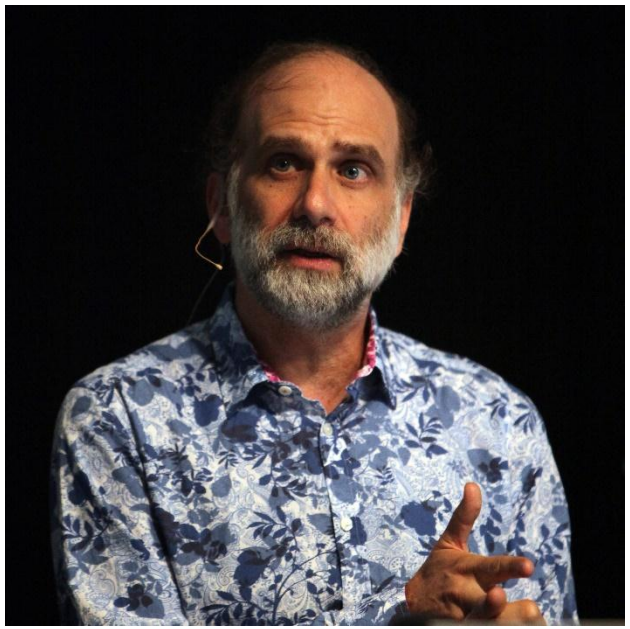
- “Всі брешуть”
- Неуважність
- Необережність
- Цікавість/інтерес
- Брак культури



Людський фактор

- Бажання подобатися
- Ввічливість
- Бажання бути корисними
- Бажання грати роль
- Пристрасті / Комплекси / Захоплення (fb)
- **“На слабо”**

Людський фактор



Брюс Шнайдер

Only amateurs attack machines; professionals target people.

Bruce Schneier - The State of Incident Response (Black Hat 2014)

Соціальна інженерія

Soc. Eng. – акт маніпуляції для досягнення певних цілей, які можуть не бути в інтересах жертви.
(Цукерберг, Мітнік, Мавроді… ворожі ЗМІ)

Класичні підстави соц. інженерії

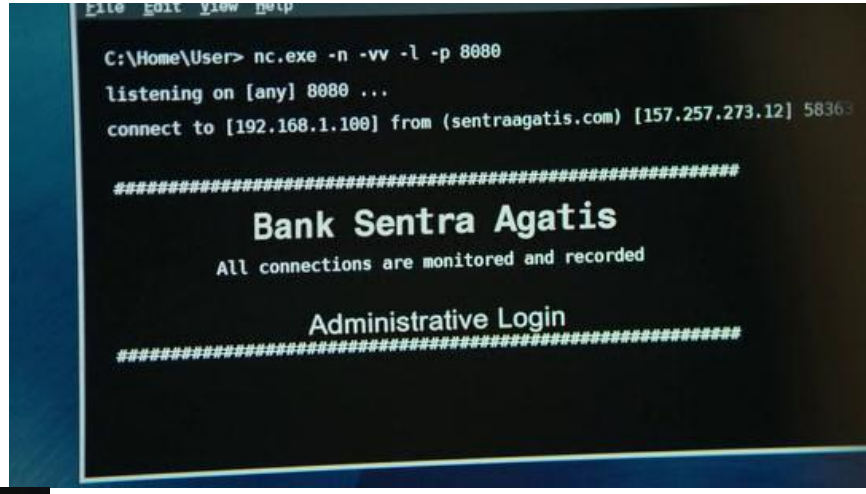
- Help Desk / Tech Support (***нагадайте ваш пароль?***)
- Співбесіда (***обидва варіанти***)
- Новий співробітник (***я тут вперше, де тут каса?***)
- Ображений/роздратований VIP замовник (***дайте мені негайно!***)
- Помилкова доставка документів (**а тут таких нема? а хто є?**)

Соціальна інженерія – приклад з кіно

Прохання роздрукувати зіпсований документ. Хіба справжній джентльмен відмовить леді ?

Соціальна інженерія – приклад з кіно

Флешка містила reverse shell, який дозволив віддалене керування скомпрометованою системою



Порушення політики ІБ

Наслідки

Соціальна інженерія – приклад з життя

Видача новин Yandex

Новости в Киеве 26 апреля, среда 00:18

1. Российский город залило реками сока из-за аварии на заводе
2. Стало известно, кто взял на себя ответственность за теракт в Питере
3. СБУ возбудила уголовное дело против иностранных политиков
4. В Киеве произошел скандал из-за вывески «Холокост-Кабаре»
5. Путин хочет начать военное сотрудничество с Украиной

Наличные курсы, продажа: **USD** 26,65 −0,08 **EUR** 28,97 0,00 ···

Новини у Києві 26 квітня, середа 00:20

1. СБУ відкрила кримінальну справу проти іноземних політиків
2. У Росії через аварію на заводі Pepsi на вулиці вилилися тонни соку
3. Стало відомо, хто стоїть за вибухами у російському метро
4. Путін заявив про готовність відновити військово-технічне співробітництво з Укра
   Важливо створити умови
5. У Києві демонтували вивіску «Голокост Кабаре» напроти синагоги

Готівкові курси, продаж: **USD** 26,65 −0,08 **EUR** 28,97 0,00 ···

Соціальна інженерія – приклад з життя

https://informnapalm.org/ua/gibrydni-vijny-pryhovana-zagroza-yandeksa-infografika/

OSINT, робота з інформацією

OSINT – використання інформації з відкритих джерел

(*отримуємо інформацію не порушуючи закон*)

OSINT, робота з інформацією

OSINT – використання інформації з відкритих джерел

(*отримуємо інформацію не порушуючи закон*)

А якими джерелами користуєтесь ви ?

OSINT, робота з інформацією

OSINT – використання інформації з відкритих джерел

(*отримуємо інформацію не порушуючи закон*)

- Google, LinkedIn, Facebook etc
- Maltego, FOCA
- Archive.org

Робота з інформацією

ІНФОРМАЦІЯ

Робота з інформацією

Робота з інформацією

Робота з інформацією

Робота з інформацією

Робота з інформацією

Робота з інформацією

Ознаки не достовірної інформації:

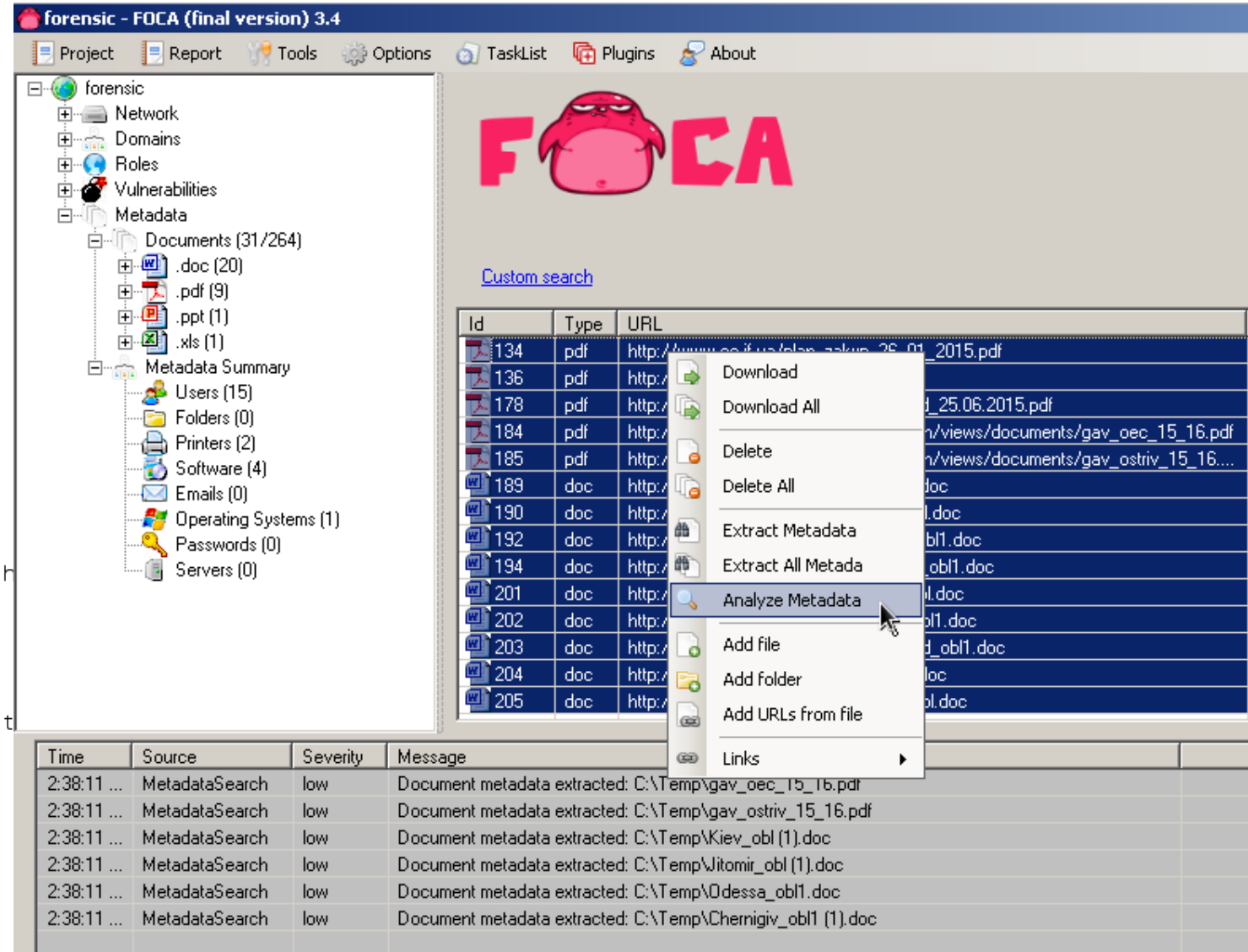
- Відсутнє чітке посилання на першоджерело
- Відсутнє підтвердження
- Картинка подана неповністю або спотворена

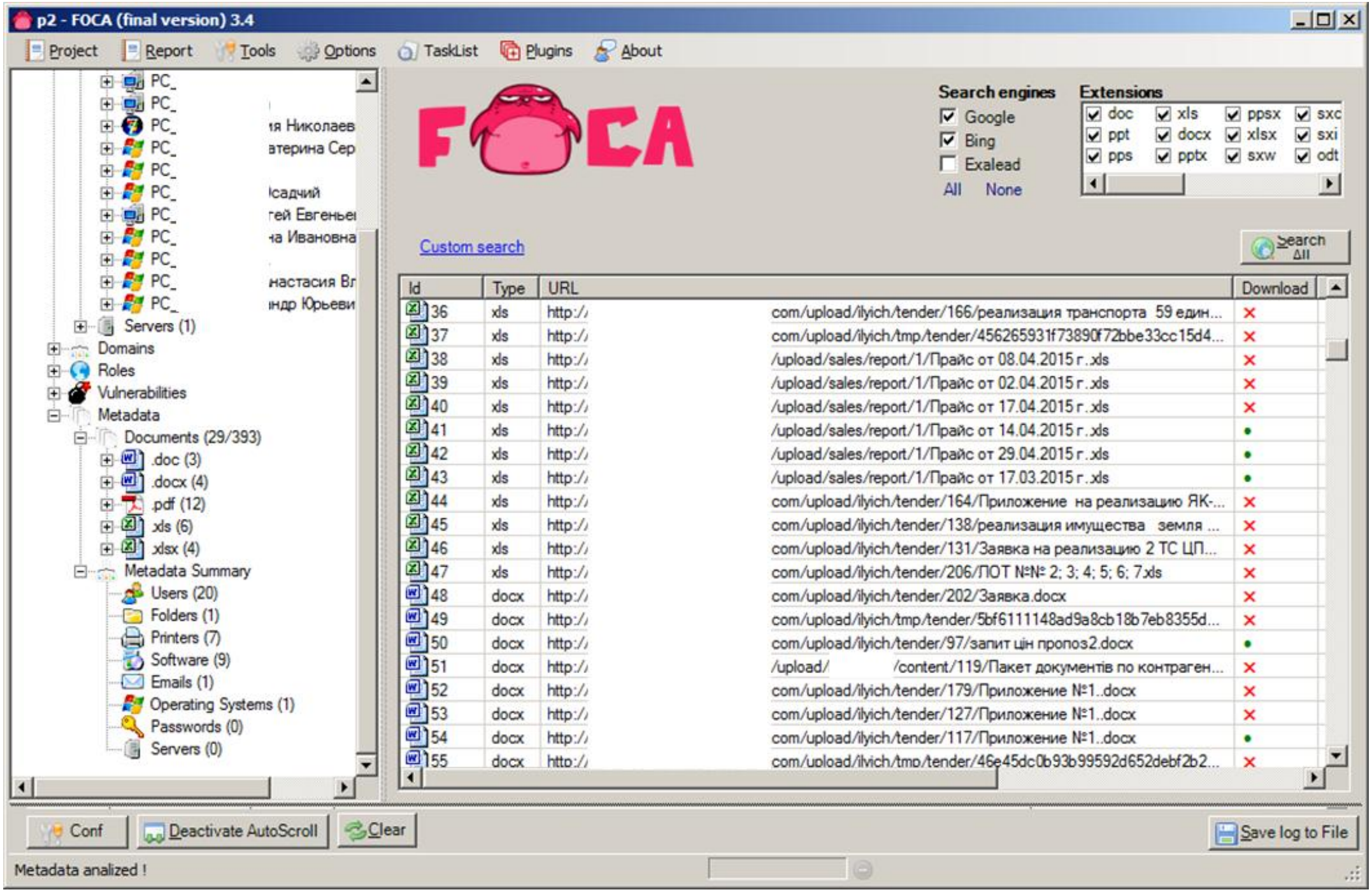
Приклади

- UAReview vs Інтерфакс, Папуги наркомани vs Телефон Яценюка
- Реклама (каріес, волосся, калгон)
- http://www.stopfake.org/kak-raspoznat-fejk/

Документи, метаінформація...

```
*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___|  \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Usage: theharvester options

       -d: Domain to search or company name
       -b: data source: google, googleCSE, bing, bingapi, pgp
                        linkedin, google-profiles, people123, jigsaw,
                        twitter, googleplus, all

       -s: Start in result number X (default: 0)
       -v: Verify host name via dns resolution and search for virtual h
       -f: Save the results into an HTML and XML file
       -n: Perform a DNS reverse query on all ranges discovered
       -c: Perform a DNS brute force for the domain name
       -t: Perform a DNS TLD expansion discovery
       -e: Use this DNS server
       -l: Limit the number of results to work with(bing goes from 50 t
       -h: use SHODAN database to query discovered hosts
            google 100 to 100, and pgp doesn't use this option)

Examples:
        theharvester -d microsoft.com -l 500 -b google
        theharvester -d microsoft.com -b pgp
        theharvester -d microsoft -l 200 -b linkedin
        theharvester -d apple.com -b googleCSE -l 500 -s 300
```




p2 - FOCA (final version) 3.4
Project
Report
Tools
Options
TaskList
Plugins
About
Search engines
Google
Bing
Exalead
All
None
Extensions
doc
xls
ppsx
sxc
ppt
docx
xlsx
sxi
pps
pptx
sxw
odt
Custom search
Search All
Id
Type
URL
Download
Servers (1)
Domains
Roles
Vulnerabilities
Metadata
Documents (29/393)
.doc (3)
.docx (4)
.pdf (12)
.xls (6)
.xlsx (4)
Metadata Summary
Users (20)
Folders (1)
Printers (7)
Software (9)
Emails (1)
Operating Systems (1)
Passwords (0)
Servers (0)
Conf
Deactivate AutoScroll
Clear
Save log to File
Metadata analized !

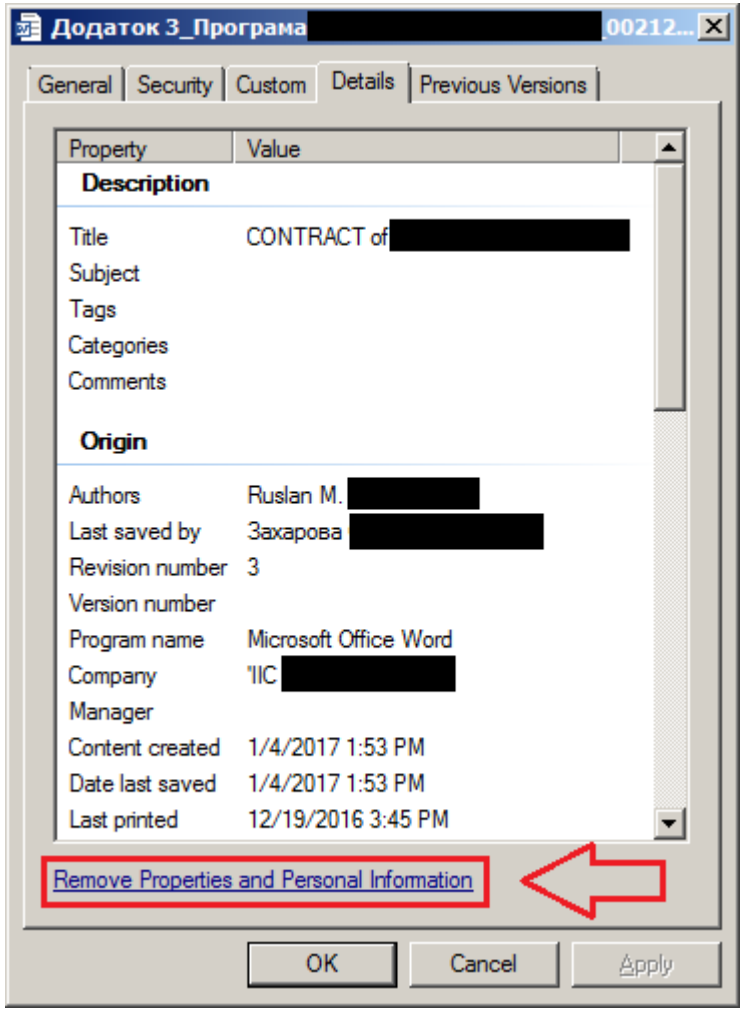
```
VRad@GK17:~$ theharvester -d [redacted].lviv.ua -l 50 -b bing

*******************************************************************
*                                                                 *
* | |_| |__   ___     /\  /\__ _ _ ____   _____  ___| |_ ___ _ __   *
* | __| '_ \ / _ \   / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|  *
* | |_| | | |  __/  / __  / (_| | |   \ V /  __/\__ \ ||  __/ |     *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Bing:
        Searching 50 results...


[+] Emails found:
------------------
@[redacted].lviv.ua
info@[redacted].lviv.ua
nfo@[redacted].lviv.ua

VRad@GK17:~$ theharvester -d [redacted].lviv.ua -l 50 -b linkedin

[-] Searching in Linkedin..
        Searching 100 results..
Users from Linkedin:
====================
Olena [redacted]
Oleksiy [redacted]
```

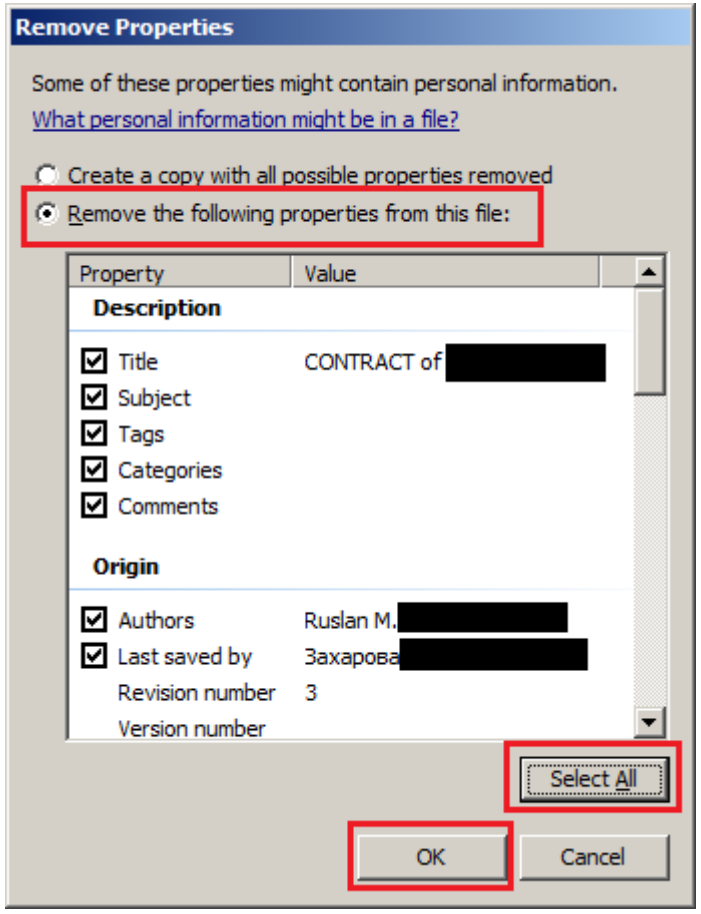
Документи, метаінформація…

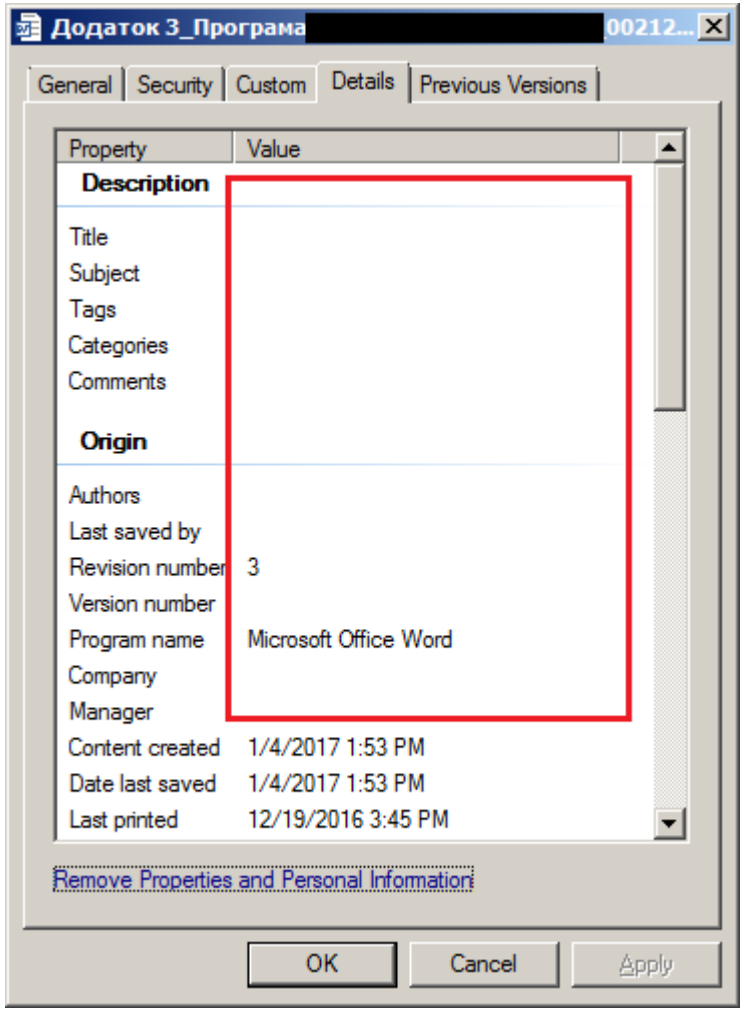
- Документи MS Office та інших форматів можуть містити **метаінформацію**
- Не говорячи про зміст документу можна отримати:
  - ім'я автора
  - ім'я системи (!) перевірка запуску
  - електрону адресу
  - мережеві принтери
  - тип ПЗ та ОС (!) експлойти
- **Видаляйте метаінформацію** перед тим як публікувати/пересилати !!!

Документи, метаінформація…

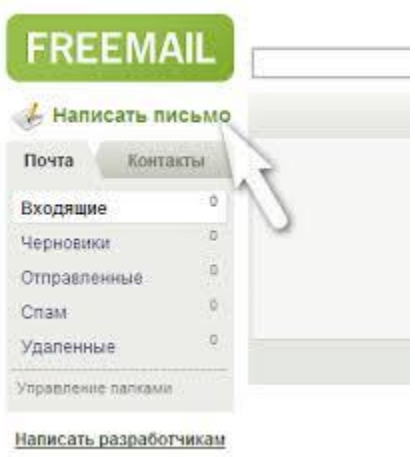
Видаляйте метаінформацію перед тим як публікувати/пересилати !!!







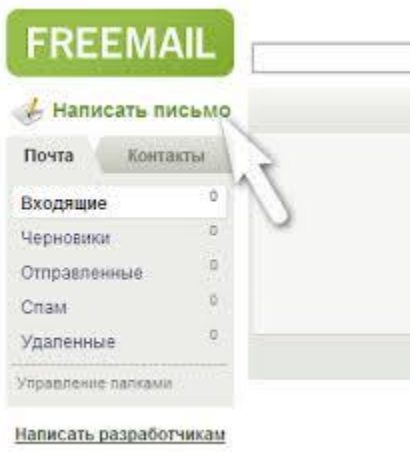
Документи і безкоштовні webmail



Webmail не є сховищем для документів !

У разі компрометації зловмисник може отримати доступ до усієї переписки, яка часто зберігається **роками !**

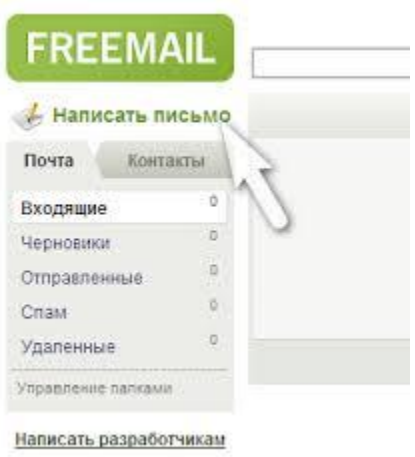
Документи і безкоштовні webmail

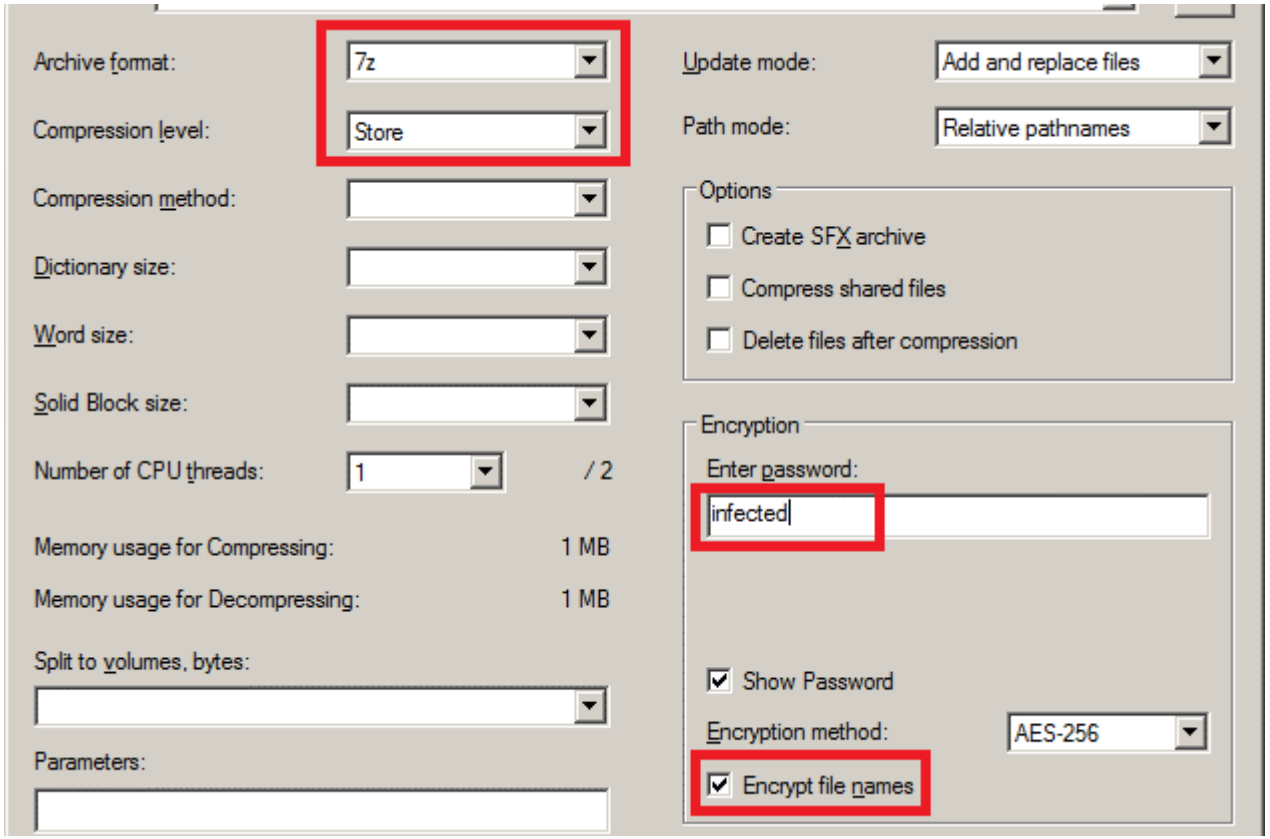


Документи захищені настільки, наскільки:

- Ви бережете пароль від сервісу
- Наскільки обережним є ваш адресат

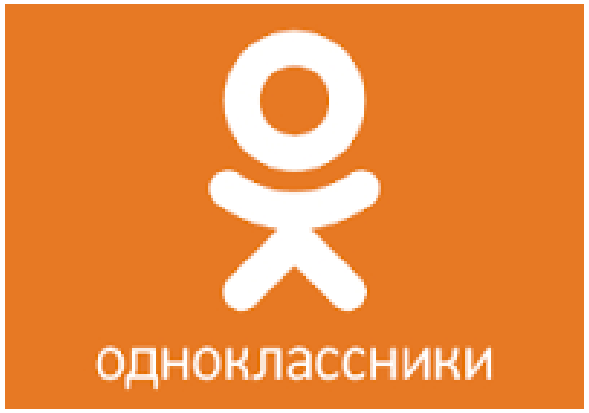
Документи і безкоштовні webmail





Якщо вже виникає потреба надіслати документ через безкоштовний сервіс пошти – не полінуйтесь заархівувати документ із паролем. Архів – у приєднання. **Пароль – по SMS.**

Сервіси від яких варто **відмовитися**



Передавати через ці канали робочу/особисту інформацію не можна!

Трохи прикладів свіжих атак

Одна із небезпек таких атак – звичайний антивірус не захищає.

Сигнатури НЕ встигають

VT

virustotal

SHA256: 41c4c60186bd6169080487ac7d68d118b4a1e48fbe3acc067551790a8795b26c

File name: mesdoc[1].exe

Detection ratio: 3 / 60

Analysis date: 2017-04-18 08:53:30 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9999	20170418
Endgame	malicious (moderate confidence)	20170413
Qihoo-360	HEUR/QVM41.1.8FEA.Malware.Gen	20170418
Ad-Aware	✓	20170418
AegisLab	✓	20170418
AhnLab-V3	✓	20170417
Alibaba	✓	20170418
ALYac	✓	20170418
Antiy-AVL	✓	20170418
Arcabit	✓	20170418
Avast	✓	20170418
AVG	✓	20170418
Avira (no cloud)	✓	20170418

VT

virustotal

SHA256:	7b72e611fd44d39e1ce7429134c3b04eaaccb23f15f589361a390a1f0d3265de
File name:	img_28962472365_mms_.jpg.zip
Detection ratio:	9 / 57
Analysis date:	2017-05-11 10:00:57 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
AegisLab	Suspar.Gen!c	20170511
Avira (no cloud)	HEUR/Suspar.Gen	20170511
Comodo	Heur.Dual.Extensions	20170511
DrWeb	JS.DownLoader.1225	20170511
Ikarus	Win32.Outbreak	20170511
K7AntiVirus	Trojan (004dfe6d1)	20170511
K7GW	Trojan (004dfe6d1)	20170510
Sophos	Mal/DrodZp-A	20170511
ZoneAlarm by Check Point	HEUR:Trojan-Downloader.Script.Generic	20170511
Ad-Aware	✓	20170511
AhnLab-V3	✓	20170511
Alibaba	✓	20170511
ALYac	✓	20170511
Antiy-AVL	✓	20170511
Arcabit	✓	20170511

VT

virustotal

SHA256: a32dfdabd1e9747e434259220405489bbcc05798bdba57e472ccb7327b9af6ad

File name: img_20093847768_mms_.jpg.js

Detection ratio: 1 / 56

Analysis date: 2017-05-11 10:01:31 UTC (0 minutes ago)

Analysis | Additional information | Comments | Votes

Antivirus	Result	Update
Ikarus	Win32.Outbreak	20170511
Ad-Aware	✓	20170511
AegisLab	✓	20170511
AhnLab-V3	✓	20170511
Alibaba		20170511
ALYac	✓	20170511
Antiy-AVL	✓	20170511
Arcabit	✓	20170511
Avast	✓	20170511
AVG	✓	20170511
Avira (no cloud)	✓	20170511
AVware	✓	20170511
Baidu	✓	20170503
BitDefender	✓	20170511
Bkav	✓	20170511

Типова схема атаки

Зловмисники запускають розсилку фішингових листів із приєднаннями. Текст листів підштовхує жертву запустити/відкрити приєднання.

Типова схема атаки

Якщо жертва відкрила приєднання та активувала приманку – завантажується чи запускається 1ша частика

Типова схема атаки

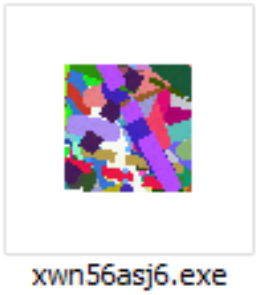
Перша частина перевіряє параметри системи, змінює налаштування проксі та активує комунікацію із C&C сервером

Типова схема атаки

xwn56asj6.exe

Завантажує з C&C сервера
модуль шифрування або віддаленого
керування (RAT)

Типова схема атаки



Функції, які можуть виконуватись другою частиною:

- кейлогер
- знімки екрану
- завантаження/вигрузка файлів
- запуск процесів та ін.

Що нового / що змінилося ?

DURANADYASAVCHENKO.RU

47.91.77.236

BELKAVKOLISEINC.RU

Що нового / що змінилося ?

- Використовують посилання (URL) замість приєднань
- Сервер з якого завантажується друга частина = сервер контролю
- **Замість макросів частіше присилають .JS , .JSE, .VBS etc**
- Замість %temp% запуск іде із каталогу профіля %AppData%
- Посилання лишаються, файли змінюються щогодини

Приклади розсилок

Wed 1/20/2016 8:20 AM

[redacted]

УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025

To [redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Message Ocenka.xls (816 KB)

Відповідно до положень Закону України «Про засади функціонування ринку електричної енергії України» та «Порядку підготовки Системним оператором плану розвитку Об'єднаної енергетичної системи України на наступні десять років», затвердженого наказом Міністерства енергетики та вугільної промисловості України від 29.09.2014 № 680, системним оператором було розроблено та розміщено на офіційному сайті компанії проект «Плану розвитку ОЕС України на 2016 – 2025 роки».

Проект Плану розвитку знаходиться в додатку до листа.

На виконання пункту 5 положення Порядку підготовки 20 січня 2016 року о 14-00 в адміністративному приміщенні ПС 750 кВ «Київська» (Київська область, Макарівський район, с. Наливайківка, вул. Жовтнева, 112-Б) будуть проводитись громадські обговорення та консультації щодо проекту Плану розвитку.

Wed 3/29/2017 11:35 AM

Державна фіскальна служба України <fillipp@aaeaerospace.com> ?!

[spam] виставлений новийрахунок

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

Добрий день !

Ви маєте ознайомитися з новим рахунком до сплати!
Дізнатися більше ви можете на нашому сайті:

https://sta-sumy.gov.ua/downloads/2017-03/423sZ98x3.html?tm=521354

http://babytlt.ru/administrator/components/com_hikashop/extensions/plg_hikashopshipping_fedex/documents.zip
Click to follow link

!!!

Якщо у Вас виникли питання Ви можете зв'язатися з нами за телефонами, вказаними на нашому сайті.

З повагою,заступник керівника державної фіскальної служби України

«Державна фіскальна служба України» Тел.: 0-800-501-007 (безкоштовно зі стаціонарних телефонів)
(044) 454-16-13 для мешканців м. Києва
04053, м. Київ, Львівська пл., буд. 8

Пн 03.04.2017 17:50

Дмитренко И.В. <slrda@slavuta-rda.gov.ua>

Звіт за 1й квартал, таблиця щокварталу аналізу

Кому [redacted]

Это сообщение было отправлено с важностью: Высокая.

Сообщение | Звіт по 1й квартал_табліца щокварталу аналізу.tar (25 Кбайт)

Доброго дня.
Список відсканованих документів:
1. Звіт за 1-й квартал 2017р.
2. Таблиці щоквартального аналізу по підприємству
С повагою, Дмитренко Ігор Валентинович

Ср 05.04.2017 16:19

ТОВ "Тепло Буд" <office@dcci.org.ua>

Виписка з реєстру, договір к-п від 4-го

Кому

Это сообщение было отправлено с важностью: Высокая.

Сообщение | Договір купівлі продажу від 4_04_17р RAR.tar (25 Кбайт)

Доброго дня. Пересилаю список відсканованих документів на прохання керівника.
1. копія договору
2. виписка з реєстру організації
З повагою гл. бух. Толочин Анастасія

ТОВ "Тепло Буд"
м. Київ, вул. Якутська, 8
Тел. (044) 489-52-67

Пн 19.05.2014 20:11

noreply@[redacted]

Scanned image from MX-2600N

Кому [redacted]

Мы удалили дополнительные разрывы строк в сообщении.

14.229.208.80
static.vnpt.vn
Hanoi
Vietnam

Сообщение | noreply@[redacted]20170410_785791.zip (72 Кбайт)

Name	Size	Packed Size	Modified	Created
20170410_313842.docm	80 038	72 818	2017-04-10 11:20	2017-04-10 11:20

Reply to: noreply@[redacted]
Location: Not Set

File Format: DOC MMR(G4)
Resolution: 200dpi x 200dpi

Attached file is scanned image in DOC format.
Use Microsoft(R)Word(R) of Microsoft Systems Incorporated to view the document.

Ср 12.04.2017 7:20

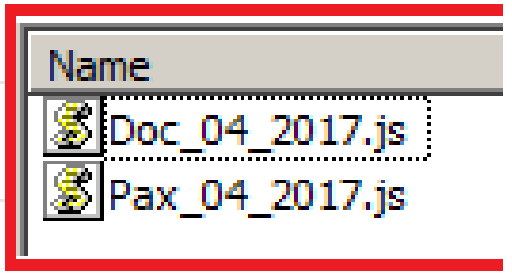
ПАТ Укртелеком <nmashina@svit-ll.com>

Інформація щодо розрахунків

Кому [redacted]

Это сообщение было отправлено с важностью: Высокая.

Сообщение | Рахунок_Scan7102000000002890_rar.tar (5 Кбайт)



--- ПОВІДОМЛЕННЯ, что пересілається ---
Від кого: ПАТ Укртелеком <Cherkaska@ukrtelecom.ua>
Тема: Інформація относительно розрахунків
Дата: 12 квітня 2017, 6:32:46

Шановний Абонент
У вкладеному файлі направляемо виконавчий рахунок за 04/2017
З повагою, ПАТ «Укртелеком»

Пн 17.04.2017 8:27

ТОВ "МІТ ФІШ" <aturchenko@antiq.xpsweb.com>

Лист партнерам про зміну директора

Кому [redacted]

Это сообщение было отправлено с важностью: Высокая.

Сообщение | зміна документів від 14 квітня rar.tar (9 Кбайт)

Name	Size	Packed Size	Modified
IMG_0001.js	3 262	3 584	2017-04-16 14:53
IMG_0002.js	3 183	3 584	2017-04-16 14:53

З повагою
ТОВ "МІТ ФІШ"
02660,Київ,Маланюка 114-А
Альона
моб: +380986151467

47.91.77.236

Connected Sites: 7

URL	Port	Reputation
BELKAVKOLISEINC.RU	80	Medium Risk
DURANADYASAVCHENKO.RU	80	Medium Risk
DURANADYASAVCHENKO.RU/VISHINKA/MESDOC.EXE	80	Medium Risk

Пн 17.04.2017 8:32

Бондар Роман <kadry@gupri.voladm.gov.ua>

Договора К Фуд

Кому [redacted]

Это сообщение было отправлено с важностью: Высокая.

Name	Size	Packed Size	Modified
JPG_001.js	3 167	3 584	2017-04-16 14:53
JPG_002.js	3 190	3 584	2017-04-16 14:53

Сообщение | шаблон реквизиты rar.tar (9 Кбайт)

С 25.04.2017 мы переходим на новое юр лицо по всем т.т.
Ранее мы работали через два : Столица Торг и Торг К
Далее все т.т. объединим под одним – Континент Фуд.
Прошу просмотреть договора во вложении и выслать шаблоны с реквизитами для формирования договоров.

З повагою,
Бондар Роман
Категорійний менеджер
Мережа магазинів "Континент"
Україна, м.Київ, вул. Якуба Коласа, 15
03148
т: +38(066)352-55-54, +38(044)403-03-00
bondar@kontinent.ua
kontinent.ua

Connected Sites: 2

URL	Port	Reputation
DURANADYASAVCHENKO.RU	80	Medium Risk
DURANADYASAVCHENKO.RU/VISHINKA/MESDOC.EXE	80	Medium Risk

47.91.77.236

Вт 18.04.2017 10:05

ТОВ "ТК"ЕКОНОМ ПЛЮС" <Yuriy.Novodon@ms-zvyazok.km.ua>

Заказ поставщику

Кому [redacted]

Это сообщение было отправлено с важностью: Высокая.

Сообщение | Заказ поставщику № K52R001786 от 17 апреля 2017 Rar.tar (9 Кбайт)

Name	Size	Packed Size	Modified
JPEG_001.js	3 206	3 584	2017-04-17 16:02
JPEG_002.js	3 238	3 584	2017-04-17 16:02

С уважением,Семенчук Ярослава
Директор магазина № 52
ООО ТК "ЭКОНОМ ПЛЮС"
г.Украинка ул.Сосновая 6а
моб.тел. 067-333-56-62

Connected Sites: 7

URL	Port	Reputation
BELKAVKOLISEINC.RU	80	Medium Risk
DURANADYASAVCHENKO.RU	80	Medium Risk
DURANADYASAVCHENKO.RU/VISHINKA/MESDOC.EXE	80	Medium Risk

47.91.77.236

Чт 14.07.2016 19:08

Анастасія Котэнко <liam.seeger@t-online.de>

info Пропонуємо ознайомитись з належними документами

To

You forwarded this message on 14.07.2016 15:08.

Message | Позов_примірник_info.doc (40 KB)

Шановний пане/пані!

Фінансовий підрозділ Діамантбанк звертається до Вас з приводу того, що на Ваше ім'я 12.09.2015 року, за допомогою нашої послуги онлайн банкінгу, було укладено договір на терміновий кредит на суму 121 433,00 гривень.

На даний момент належну суму за кредитом не погашено. Станом на дату надсилання цього листа року Ваш борг з урахуванням пені (0,7% за кожну добу прострочення оплати) становить 51 000,59 грн.

У зв'язку з цим, на підставі кредитної угоди, керівництвом відділення було прийнято рішення про складання судового позову на Ваше ім'я.

Пропонуємо ознайомитись з відповідними документами.

Чт 14.07.2016 22:02

Онисим Миргородский <arsoy.nej@t-online.de>

office, Угоду_про_кредитування - ВТБ Банк

To

You forwarded this message on 14.07.2016 17:03.

Message | Угоду_про_видачу безготівкового_кредиту_office.doc (40 KB)

Високошановний добродію!

Юридичний підрозділ нагадує вам, що, відповідно до наявних документів, 11.12.2015 року на Ваш ідентифікаційний код було укладено кредитний договір на суму 210 000,00 гривень.

Вважаємо за свій обов'язок сповістити Вас про те, що Вашу заборгованість на сьогоднішній день досі не погашено, натомість сума продовжує зростати за рахунок процентів та штрафних санкцій, що становить 0,9% за кожен банківський день прострочення.

Оскільки Ви, всупереч умовам договору, і досі не внесли належну суму позики, ми змушені призупинити дію договору та звернутись до суду для примусового стягнення суми кредиту та штрафних санкцій.

Пропонуємо Вам ознайомитись з відповідною документацією.

P.S. Запевняємо Вас, що, якщо протягом 20 банківських днів Ви внесете на рахунок банку вказану суму заборгованості, ми й надалі співпрацюватимемо на попередніх умовах.

Правило 30 секунд

- Коли вам надходить email, не поспішайте відкривати приєднання чи посилання !

Витратьте 30 секунд щоб уважно перевірити лист:

- Знайдіть офіційний сайт організації, порівняйте номери і домени
- Чи співпадає адреса в полі “від” тій компанії про яку йдеться в самому листі?
- Чи співпадає поштова скринька із ПІБ людини яка начебто написала листа?
- Чи немає в тексті орфографічних/граматичних помилок? Відмінки?
- Чи є внизу листа корпоративний підпис?

Якщо щось викликає підозру – не нехтуйте можливістю звернутися за телефоном у підписі

і перепитати людину що саме вона вам надіслала? Як правило 90% фішингу виявляються при уважній перевірці змісту листа.

Правило 30 секунд

- Якщо лист надійшов від невідомого – перевіряйте усе по порядку

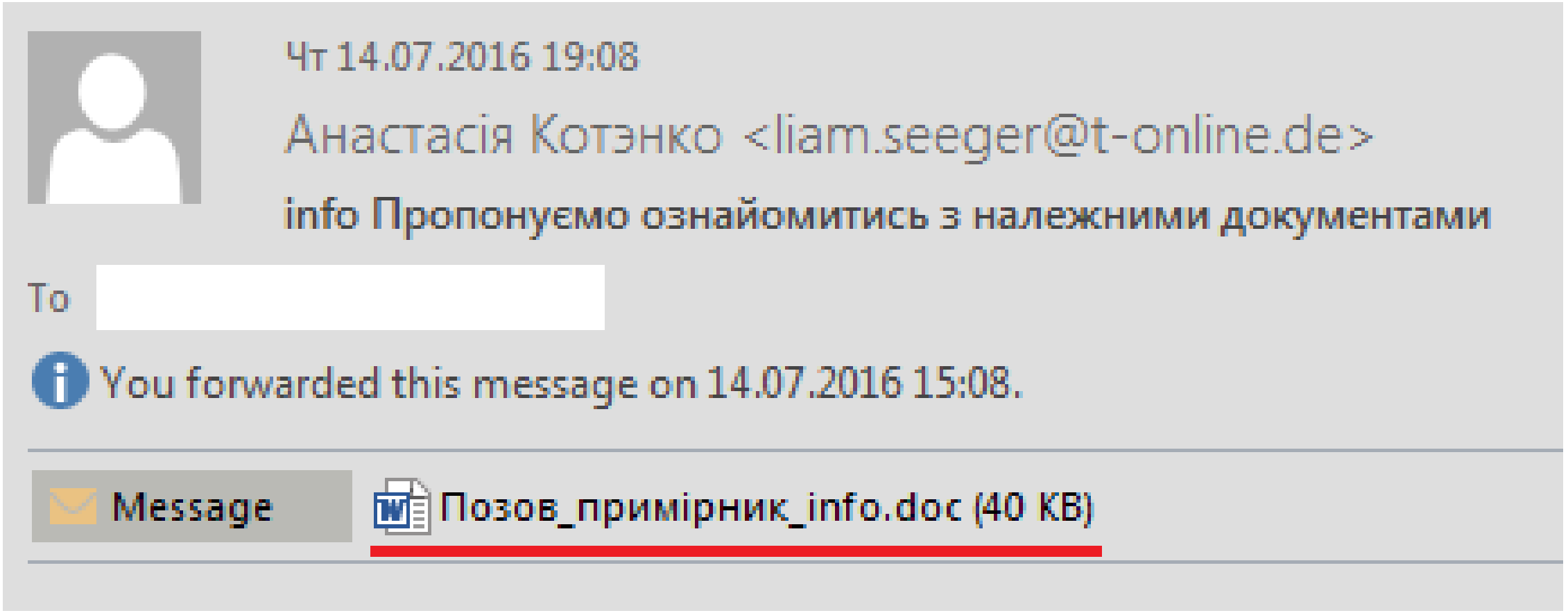
- Якщо телефон у підписі не відповідає/не дійсний – зверніться за контактами вказаними на офіційному ресурсі компанії

** На телефон у підписі фейкового листа може відповісти підставна особа.*

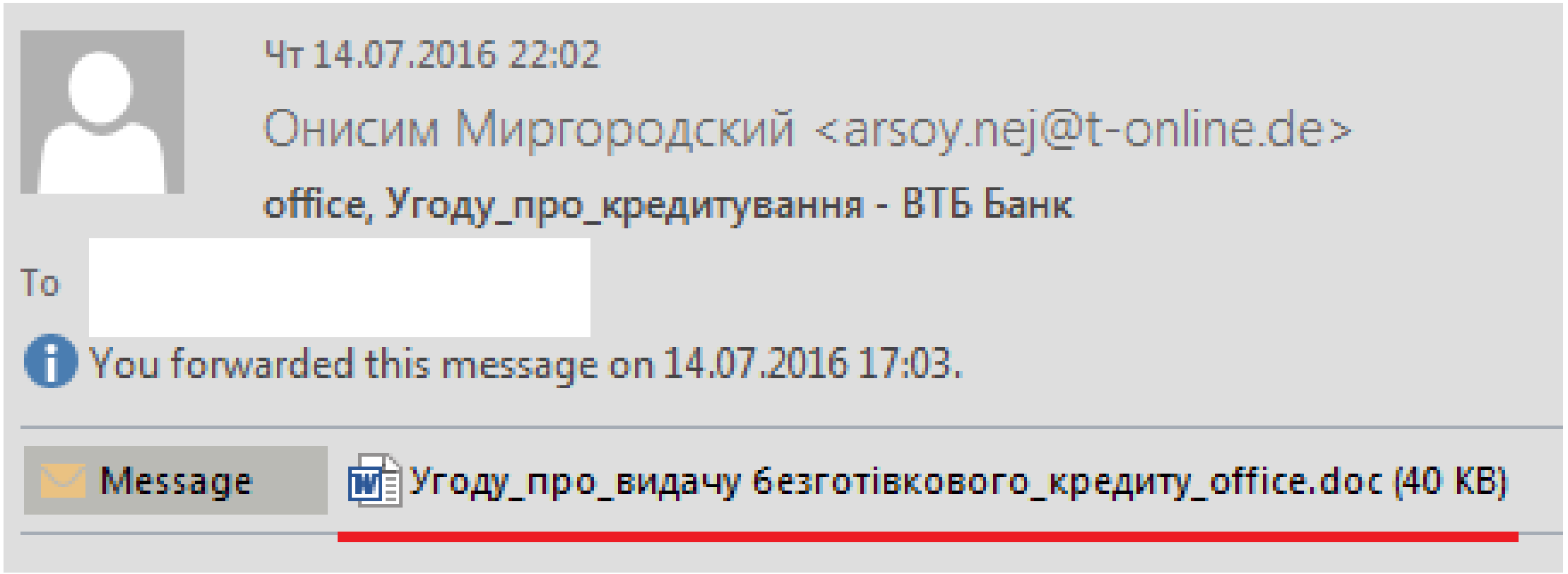
- Якщо підозрілий лист надійшов від колеги/знайомого – зв'яжіться з людиною перш ніж відкривати приєднання чи посилання

** Особливо якщо ви не очікуєте від нього якихось документів/рахунків.*

Правило 30 секунд



Правило 30 секунд



Правило 30 секунд

Вт 18.04.2017 10:05

ТОВ "ТК"ЕКОНОМ ПЛЮС" <Yuriy.Novodon@ms-zvyazok.km.ua>

Заказ поставщику

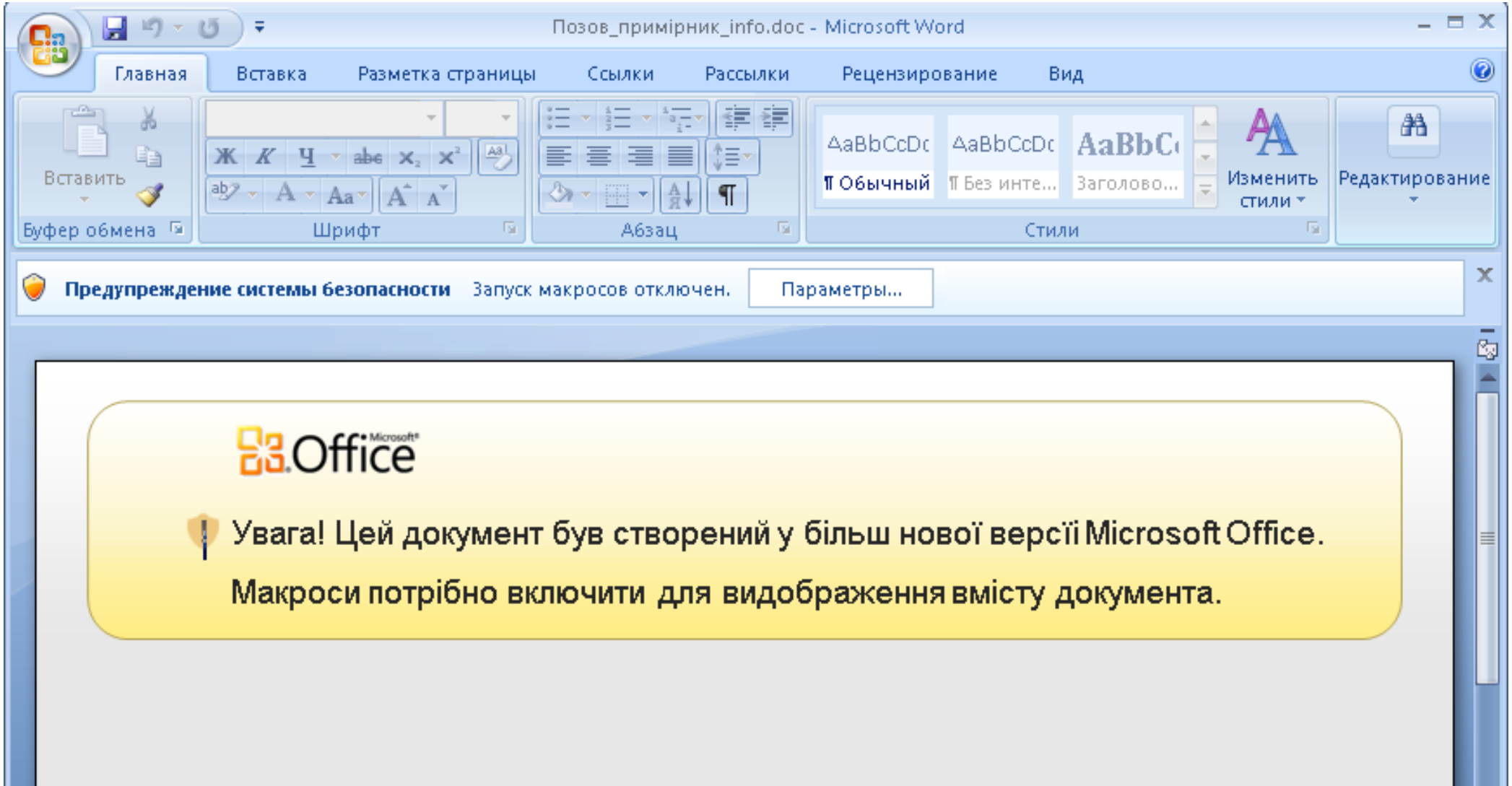
Кому [redacted]

Это сообщение было отправлено с важностью: Высокая.

Сообщение | Заказ поставщику № K52R001786 от 17 апреля 2017 Rar.tar (9 Кбайт)

С уважением,Семенчук Ярослава
Директор магазина № 52
ООО ТК "ЭКОНОМ ПЛЮС"
г.Украинка ул.Сосновая 6а
моб.тел. 067-333-56-62

НЕ АКТИВУЙТЕ МАКРОСИ!



Паролі

Gmail	Yandex	Mail.ru
123456	123456	qwerty
password	123456789	123456
123456789	111111	qwertyuiop
qwerty	qwerty	qwe123
12345678	1234567890	qweqwe
111111	1234567	klaster
abc123	7777777	1qaz2wsx
123123	123321	1q2w3e4r
1234567	000000	qazwsx
1234567890	123123	1q2w3e
iloveyou	[illegible]	123qwe
password1	[illegible]	1q2w3e4r5t
000000	[illegible]	123456789
zaq12wsx	654321	111111
tinkle	gfhjkm	zxcvbnm
qwerty123	777777	1234qwer
monkey	112233	qwer1234
target123	121212	asdfgh
dragon	987654321	marina
1q2w3e4r	159753	q1w2e3r4t5

2014

2013

Rank	Password	Change from 2012
1	123456	*Up 1*
2	password	*Down 1*
3	12345678	*Unchanged*
4	qwerty	*Up 1*
5	abc123	*Down 1*
6	123456789	*New*
7	111111	*Up 2*
8	1234567	*Up 5*
9	iloveyou	*Up 2*
10	adobe123	*New*
11	123123	*Up 5*
12	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
14	[illegible]	[illegible]
15	photoshop	*New*
16	1234	*New*
17	monkey	*Down 11*
18	shadow	*Unchanged*
19	sunshine	*Down 5*
20	12345	*New*

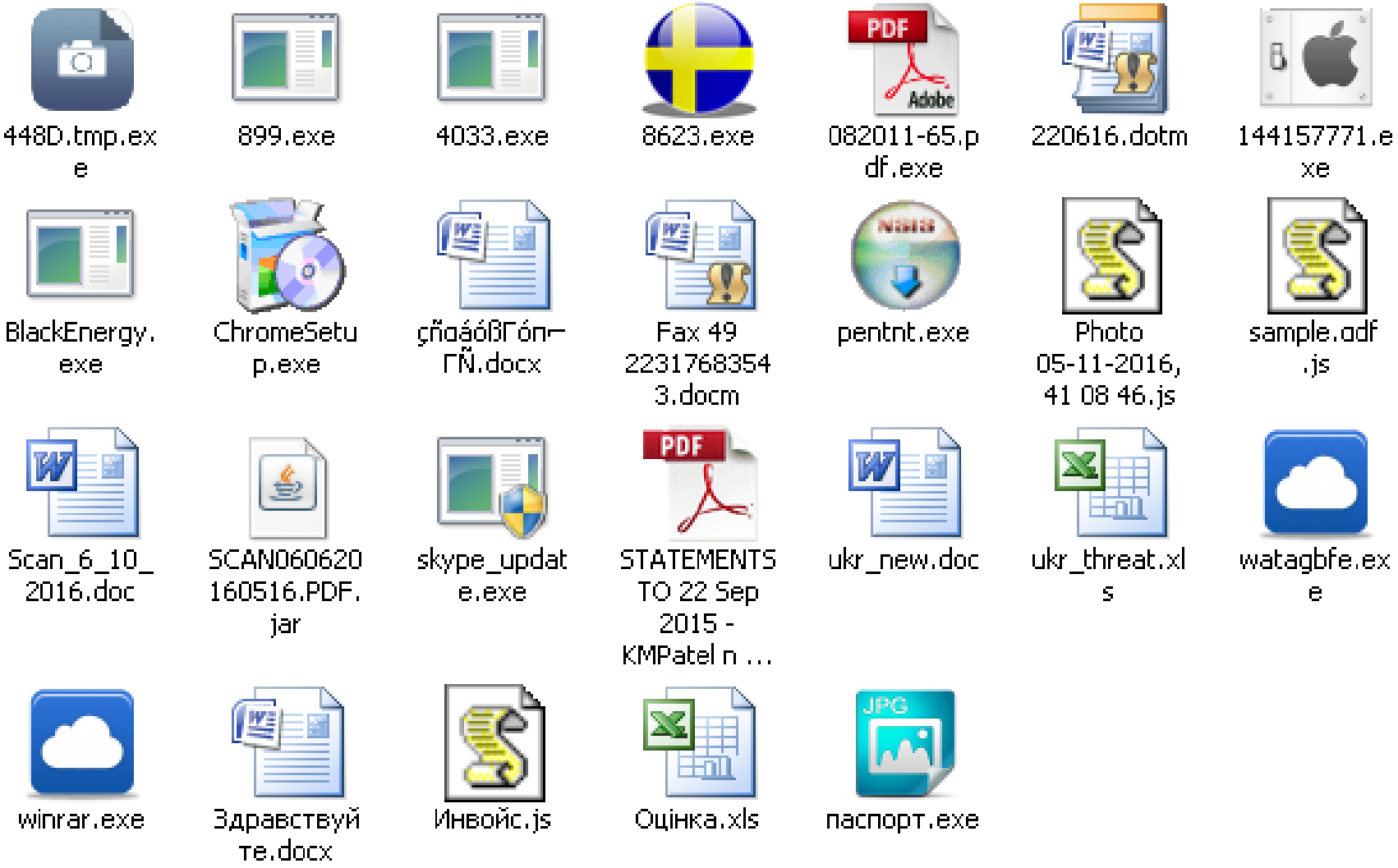
Паролі

- Паролі потрібно пам'ятати, а не зберігати у бравзерах і т.д.
- Розділіть пароль ні три категорії:
  - Робота (максимум)
  - Особисте (не слабше)
  - Сміття (розсилки, форуми на 1 раз і т. ін)
- Пароль **не повинен** включати інформацію яку ви про себе уже розповіли/запостили!
- Пароль, а радше **парольна фраза** мусить складатися із двох різних половинок
- Пароль мусить бути довжиною **від 10-12** символів
- Варто і потрібно застосовувати методи ускладнення перебору – укр. розкладку і цифри
- Приклади: _k0@L@#p@RK3r_

  %Ь»Ь)НТ!І0зк0ь»е (мамонт!сопромат)

  Е1т1_Я»иге1р_3к3вл1м№Veresen` (тіні_забутих_предків#Veresen`)

Додатки


448D.tmp.exe
899.exe
4033.exe
8623.exe
082011-65.pdf.exe
220616.dotm
144157771.exe
BlackEnergy.exe
ChromeSetup.exe
çñöáóßГón–ГÑ.docx
Fax 49 2231768354 3.docm
pentnt.exe
Photo 05-11-2016, 41 08 46.js
sample.odf.js
Scan_6_10_2016.doc
SCAN060620160516.PDF.jar
skype_update.exe
STATEMENTS TO 22 Sep 2015 - KMPatel n ...
ukr_new.doc
ukr_threat.xls
watagbfe.exe
winrar.exe
Здравствуйте.docx
Инвойс.js
Оцінка.xls
паспорт.exe

Додатки

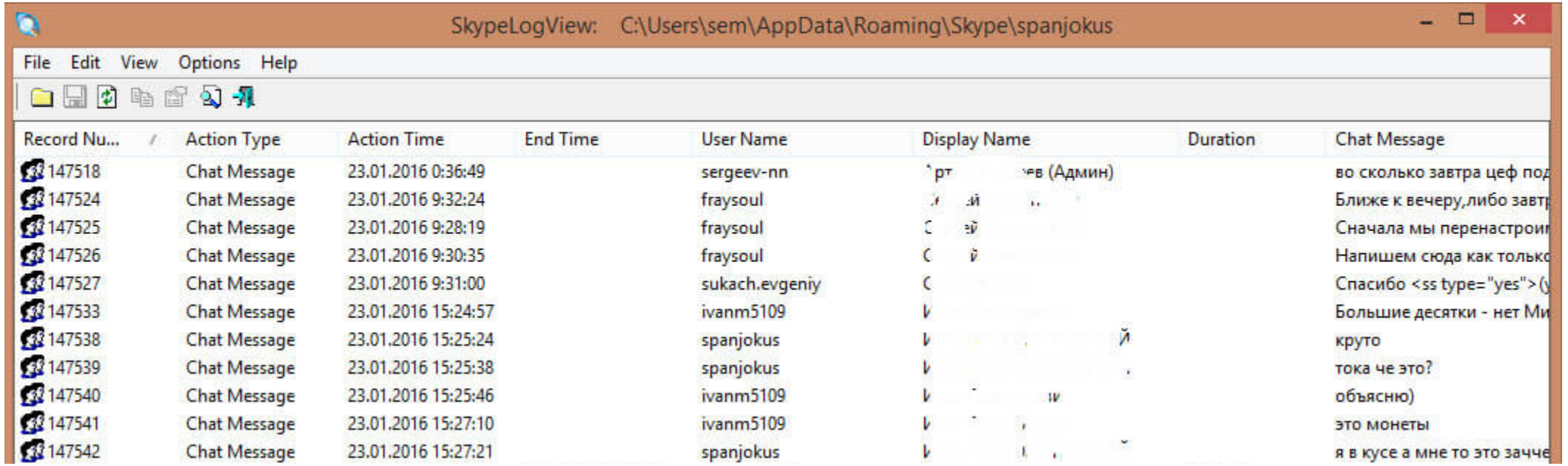
- Дистрибутиви брати **тільки** з офіційних джерел!

http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/

- Для платного/зламаного ПЗ можна пошукати альтернативу
- Не користуватися файлозвалищами!
- Своєчасно оновлювати ОС та ПЗ, особилво бравзери
- По можливості, якщо не критично відмовитись від:
  - Adobe Flash -> HTML5
  - Java RE
  - Adobe Acrobat (Reader) -> PDF Exchange Viewer

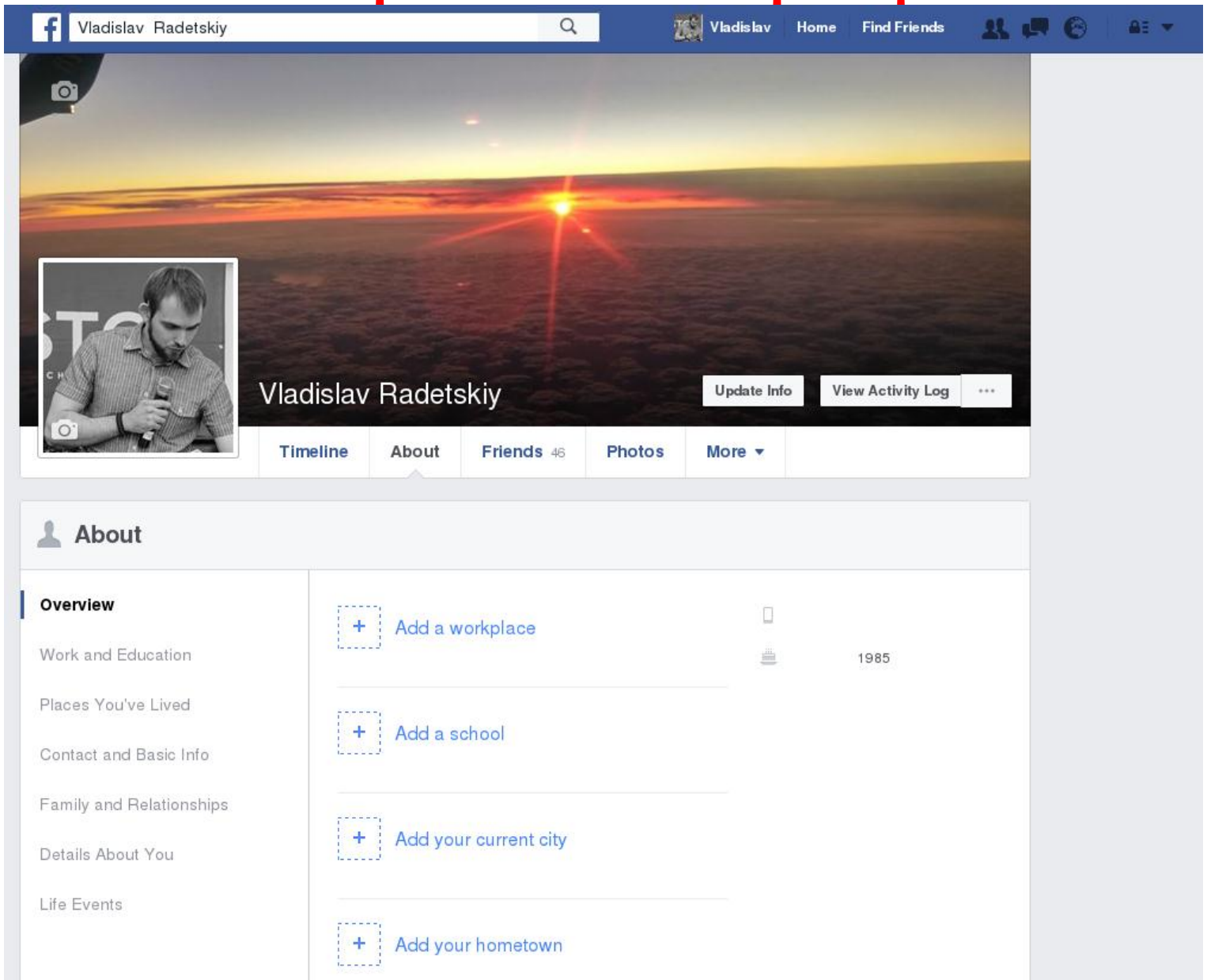
Чужі системи

- Чужа система = чорна діра
- Там можуть бути кейлоггери, трояни та інше ШПЗ
- Не залишайте своїх паролів на чужих системах
- Простий приклад зі Skype



Record Nu...	Action Type	Action Time	End Time	User Name	Display Name	Duration	Chat Message
147518	Chat Message	23.01.2016 0:36:49		sergeev-nn	рт ев (Админ)		во сколько завтра цеф под
147524	Chat Message	23.01.2016 9:32:24		fraysoul			Ближе к вечеру,либо завтр
147525	Chat Message	23.01.2016 9:28:19		fraysoul			Сначала мы перенастроим
147526	Chat Message	23.01.2016 9:30:35		fraysoul			Напишем сюда как только
147527	Chat Message	23.01.2016 9:31:00		sukach.evgeniy			Спасибо <ss type="yes">(y
147533	Chat Message	23.01.2016 15:24:57		ivanm5109			Большие десятки - нет Ми
147538	Chat Message	23.01.2016 15:25:24		spanjokus			круто
147539	Chat Message	23.01.2016 15:25:38		spanjokus			тока че это?
147540	Chat Message	23.01.2016 15:25:46		ivanm5109			объясню)
147541	Chat Message	23.01.2016 15:27:10		ivanm5109			это монеты
147542	Chat Message	23.01.2016 15:27:21		spanjokus			я в кусе а мне то это зачем

Соц. Мережі – закривайте профіль!



Intro

технічна скромняга, одна штука

Photos

Friends

Vladislav Radetskiy updated his cover photo.
October 29 at 9:13pm

Share

6

Vladislav Radetskiy
September 23

Готуємось...
See Translation

OCT 28 **Age of Security Forum 2016**
Oct 28 - Nov 4
58 people interested · 93 people going
★ Interested

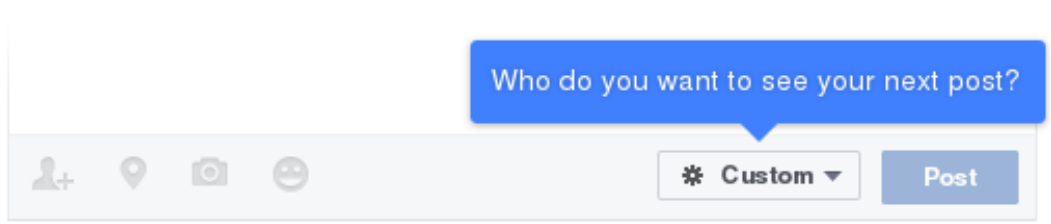
Share

Privacy Checkup

Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.

1 Posts

Whenever you post from News Feed or your profile, you can choose an audience to control who sees it.



Tip: You can change your audience each time you post.

Learn More | Next

2 Apps

3 Profile

Privacy Checkup

Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.

Great! Your future posts will be shared with the audience you have selected until you change it again. You can change this whenever you post, or on your Privacy Settings page.

2 Apps

You don't have any apps connected to your Facebook account. If you ever log into an app using Facebook, you can view it and edit the privacy in your App Settings.

Well look at that, you don't have any apps to review!

Learn More | Next

3 Profile

Privacy Checkup

Thanks for making some time for this. Now let's go through 3 steps to help make sure you're sharing with the right people.

Great! Your future posts will be shared with the audience you have selected until you change it again. You can change this whenever you post, or on your Privacy Settings page.

Keep in mind, you can review and edit your apps at any time from your app settings.

3 Profile

Have a look at this info from your profile and decide who to share it with. Remember, your profile may include more than what's here.

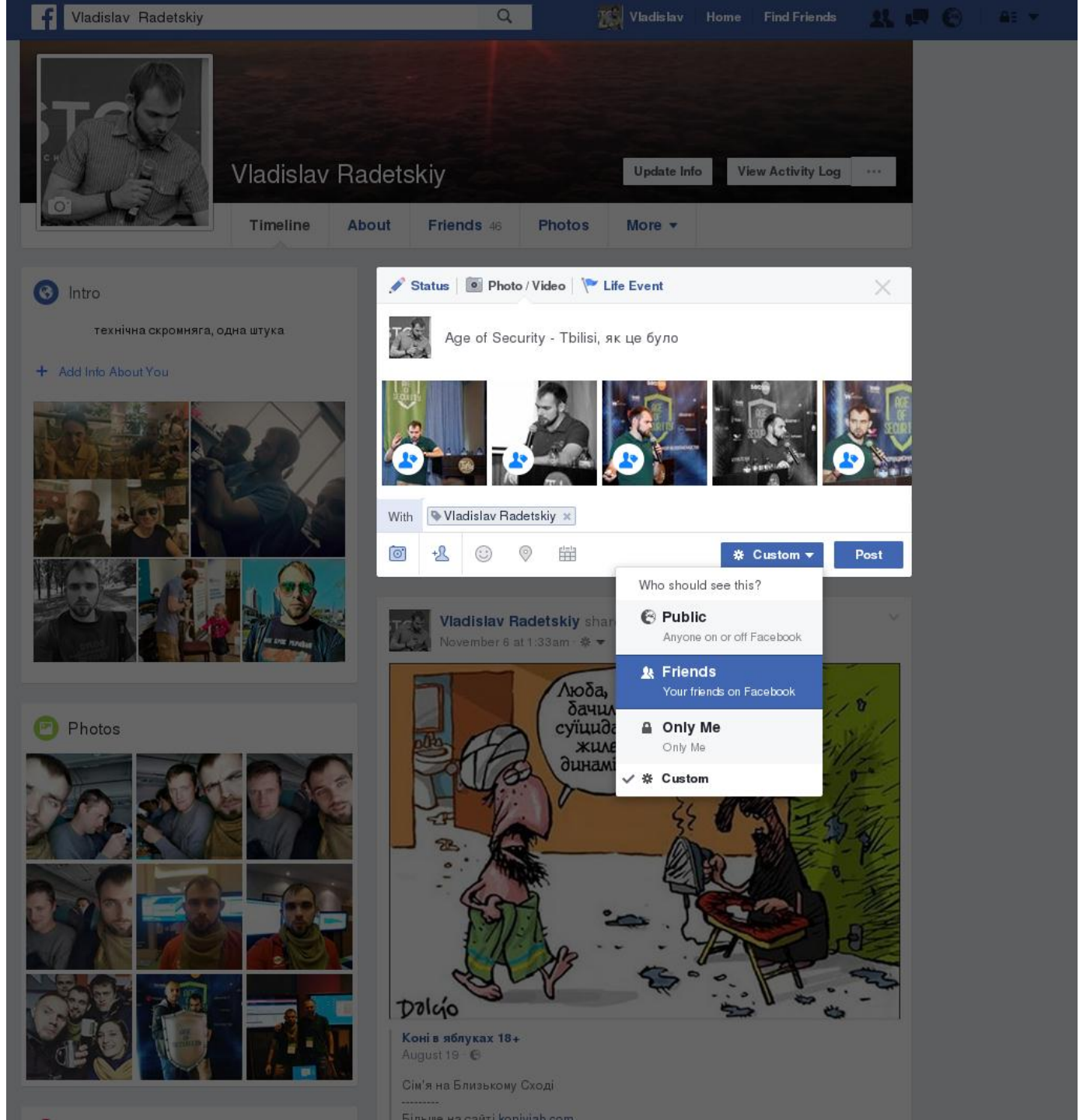
Phone
[redacted] — Only Me

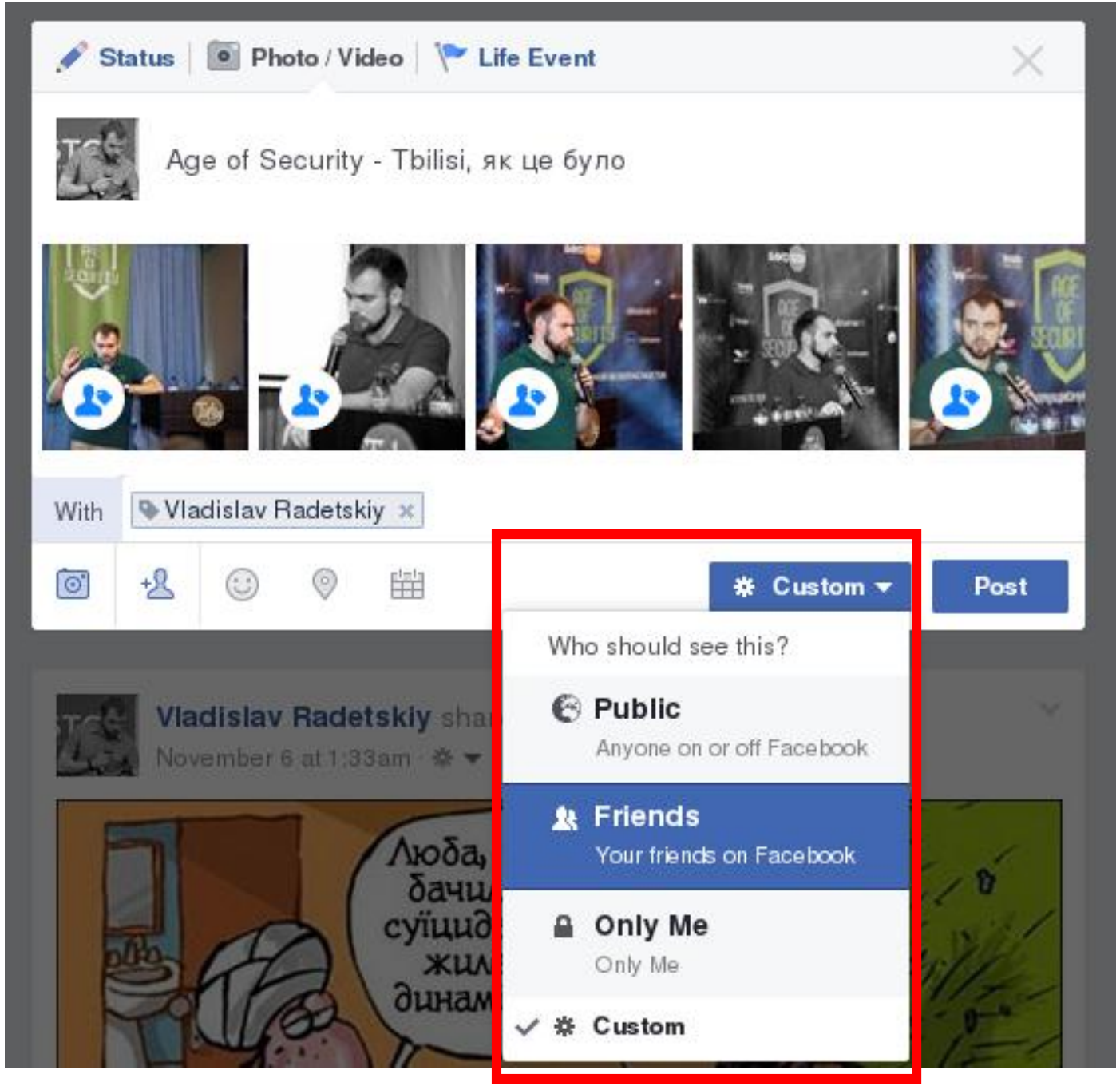
Email
[redacted] — Only Me

Birthday
[redacted] — Only Me
1985 — Friends

Tip: Go to the About section of your profile to see everything and check who you're sharing it with.

My About Page | Finish Up


Vladislav Radetskiy
Vladislav
Home
Find Friends
Vladislav Radetskiy
Update Info
View Activity Log
Timeline
About
Friends 46
Photos
More
Intro
технічна скромняга, одна штука
Add Info About You
Photos
Status
Photo / Video
Life Event
Age of Security - Tbilisi, як це було
With
Vladislav Radetskiy
Custom
Post
Who should see this?
Public
Anyone on or off Facebook
Friends
Your friends on Facebook
Only Me
Only Me
Custom
Vladislav Radetskiy
November 6 at 1:33am
Коні в яблуках 18+
August 19
Сім'я на Близькому Сході


Status
Photo / Video
Life Event
Age of Security - Tbilisi, як це було
With
Vladislav Radetskiy
Custom
Post
Who should see this?
Public
Anyone on or off Facebook
Friends
Your friends on Facebook
Only Me
Only Me
Custom
Vladislav Radetskiy
November 6 at 1:33am

Vladislav Radetskiy

Vladislav | Home 3 | Find Friends

Vladislav Radetskiy

Update Info | View Activity Log | ...

Timeline | About | Friends 46 | Photos | More

Intro

технічна скромняга, одна штука

+ Add Info About You

Photos

Status | Photo / Video | Life Event

What's on your mind?

Friends | Post

Vladislav Radetskiy added 5 new photos.
4 mins

Age of Security - Tbilisi, як це було

Like | Comment | Share

Write a comment...

Vladislav Radetskiy shared Коні в яблуках 18+'s photo.
November 6 at 1:33am

Vladislav Radetskiy

Vladislav | Home 3 | Find Friends

This is what your Timeline looks like to: Public **View as Specific Person**

Vladislav Radetskiy

Message ...

Timeline | About | Friends | Photos | More

DO YOU KNOW VLADISLAV?

If you know Vladislav, send him a message.

Intro

технічна скромняга, одна штука

Photos · Nothing to show

Friends

English (US) · Українська · Русский · Español · Português (Brasil) +

Privacy · Terms · Advertising · Ad Choices · Cookies · More

Facebook © 2016

Vladislav Radetskiy updated his cover photo.
October 29 at 9:13pm

Share

6

Vladislav Radetskiy
September 23

Готуємось...

See Translation

Висновки

1) Будьте обережними та уважними при роботі з IT
2) Пам'ятайте те, за що вас можна зачепити
3) Не сидіть під обліковим записом admin/root, не вимикайте UAC (!)
3) Вчасно оновлюйте додатки
4) Не забувайте про VirusTotal!
6) Система без Java, Flash та Adobe Reader? + 77 до карми
7) Не залишайте власних слідів на чужих системах (*паролі, облікові записи..*)
8) Не пускайте аби-кого за свої системи (“*подивитись пошту*” *тощо*)
9) Не передавайте документи по відкритим каналам
10) Уважно обирайте засоби комунікації
11) Змініть паролі від своїх систем/облікових записів

Безпека держави залежить від вчинків кожного з нас