



# Особиста безпека в Internet

**СТАНІСЛАВ САМОЙЛОВ**

Головний інспектор УІТП Департаменту кіберполіції України Національної поліції України

# ЗАГАЛЬНА СТРУКТУРА ДКП



Відділ моніторингу, відділ аналітичного забезпечення,  
відділ електронної комерції,  
відділ платіжних систем, відділ нелегального контенту,  
НКП 24/7, відділ кібербезпеки,  
управління інформаційних технологій та програмування



# Як дурять у мережі Internet



## ФІШИНГ

(англ. phishing МФА: ['fɪʃɪŋ] від fishing — рибальство) — вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів, соціальних мереж, месенджерів тощо.



# Реальні приклади (із практики)



## CASE №1

У співпраці із правоохоронними органами Франції, Німеччини, Великобританії, США та ін., розслідували факти крадіжки аутентифікаційних даних користувачів Apple



# CASE #1 (дослідження)



```
Interface: USB  
Model: SanDisk U3 Cruzer Micro  
Firmware revision: 3.27  
USB Serial number: 0000185E2574F810  
Capacity in bytes: 4,100,980,736 (4.1 GB)  
Block Size: 512 bytes  
Block Count: 8,009,728
```

Об'єкт дослідження

Технічна (ідентифікуюча)  
інформація про носій





# CASE #1 (дослідження)

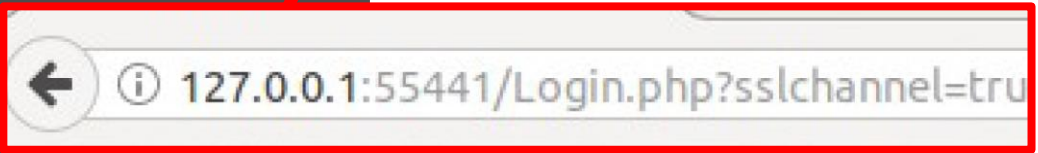
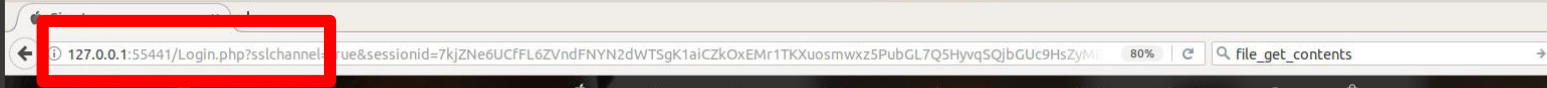


Після застосування ряду «магічних» заклять....

У броузері Firefox було відкрито сторінку за посиланням

<http://127.0.0.1:55441/index.php>

(127.0.0.1 – локальна адреса комп'ютера)



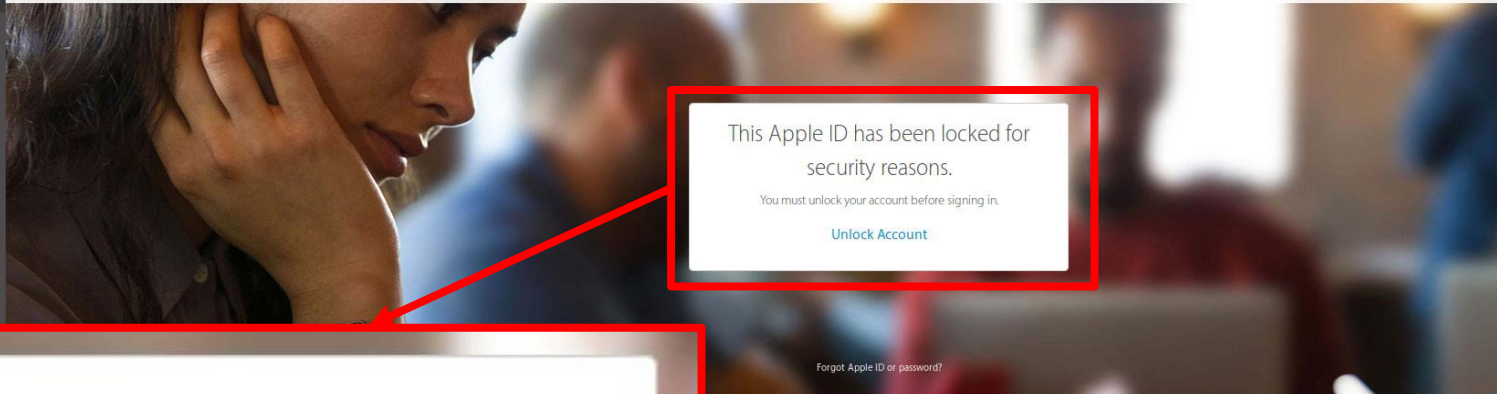
## Your account for everything Apple.

A single Apple ID and password gives you access to all Apple services.  
[Learn more about Apple ID >](#)



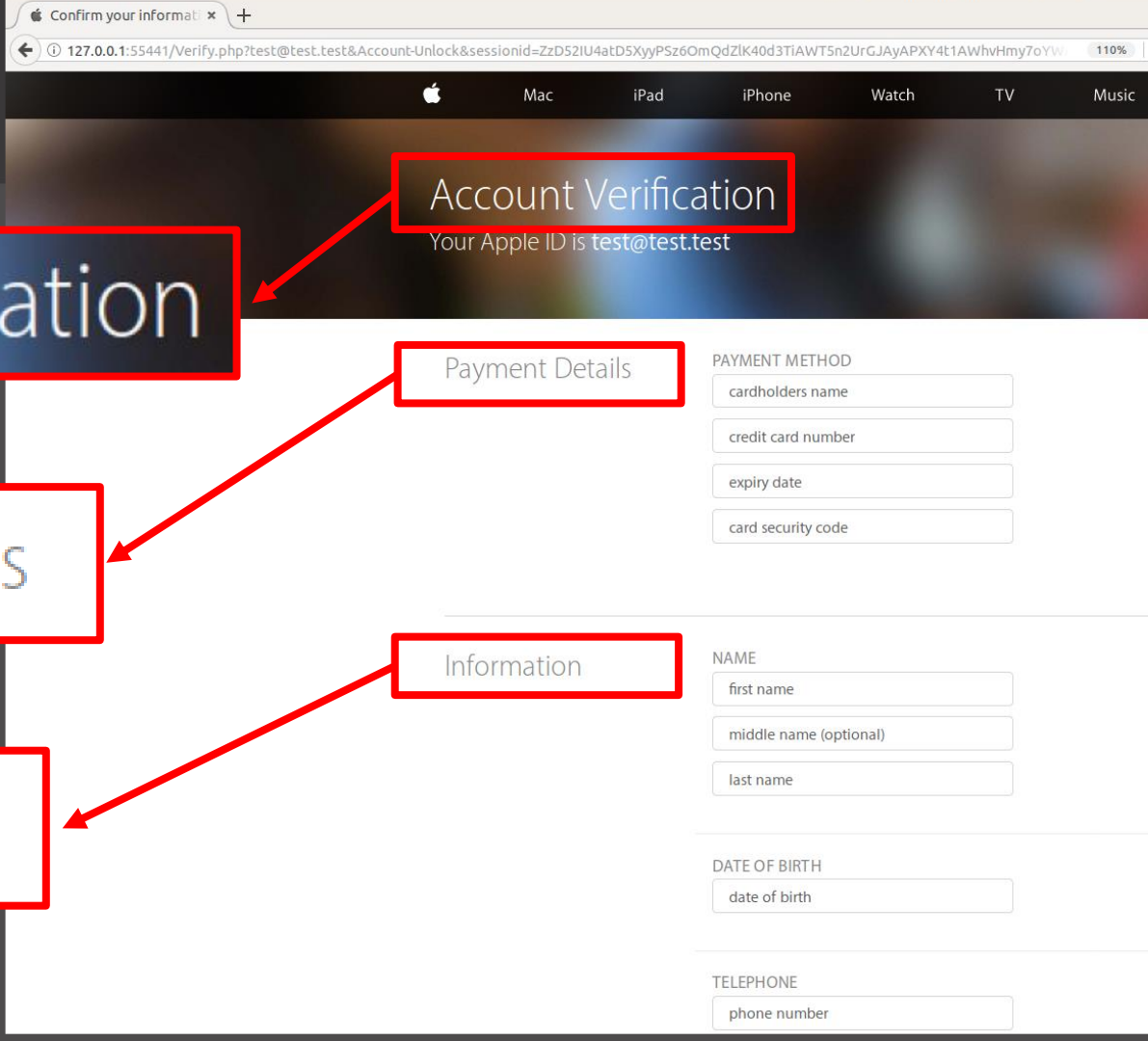
[Create your Apple ID >](#)





This Apple ID has been locked for security reasons.  
You must unlock your account before signing in.  
[Unlock Account](#)

This Apple ID has been locked for security reasons.  
You must unlock your account before signing in.  
[Unlock Account](#)



Account Verification

Payment Details

Information

Account Verification

Your Apple ID is test@test.test

Payment Details

PAYMENT METHOD

cardholders name  
credit card number  
expiry date  
card security code

Information

NAME

first name  
middle name (optional)  
last name

DATE OF BIRTH

date of birth

TELEPHONE

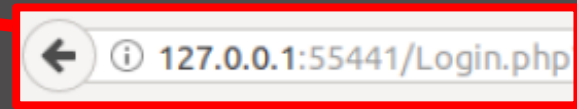
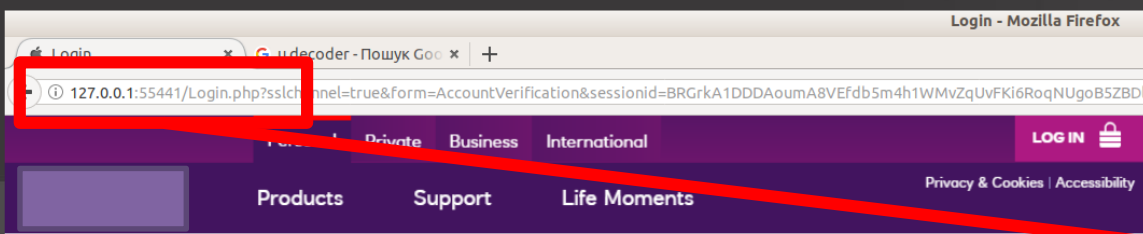
phone number

# Реальні приклади (із практики)



## CASE №2

Крадіжка аккаунтів електронного банкінгу



## Online Banking services

Online banking **Credit card services**

### Welcome to Online Banking

Customer number  [Forgotten any of your log in details?>](#)

This is your date of birth (ddmmyy) followed by your unique number which identifies you to the bank.

Remember me. We don't recommend storing data on a shared computer.

[Tell me more about this feature>](#)

[Log in](#)

[Not an online user? Sign up here>](#)



**Fraudsters call pretending to be the bank and other companies you trust.**

If in doubt hang up, search for a number you can trust, and call back to confirm what is being asked. Remember, we will never ask for your full PIN, full password or card reader information.

Only individuals who have a NatWest account and authorised access to Online Banking should proceed beyond this point. For the security of customers, any unauthorised attempt to access customer bank information will be monitored and may be subject to

Досліджували за алгоритмом, що описувався вище

# Digital Banking

## Log In – Step 2

### Your security number

Enter the following numbers from your security number

Enter the 4th number

Enter the 2nd number

Enter the 3rd number

### Your password

Enter the following characters from your password

Enter the 1st character

Enter the 2nd character

Enter the 3rd character

[Forgotten your security number or password?>](#)


### Users with Special Needs

Do not refresh my screen on timeout.

[Explain our timeout feature>](#)

Back

Next

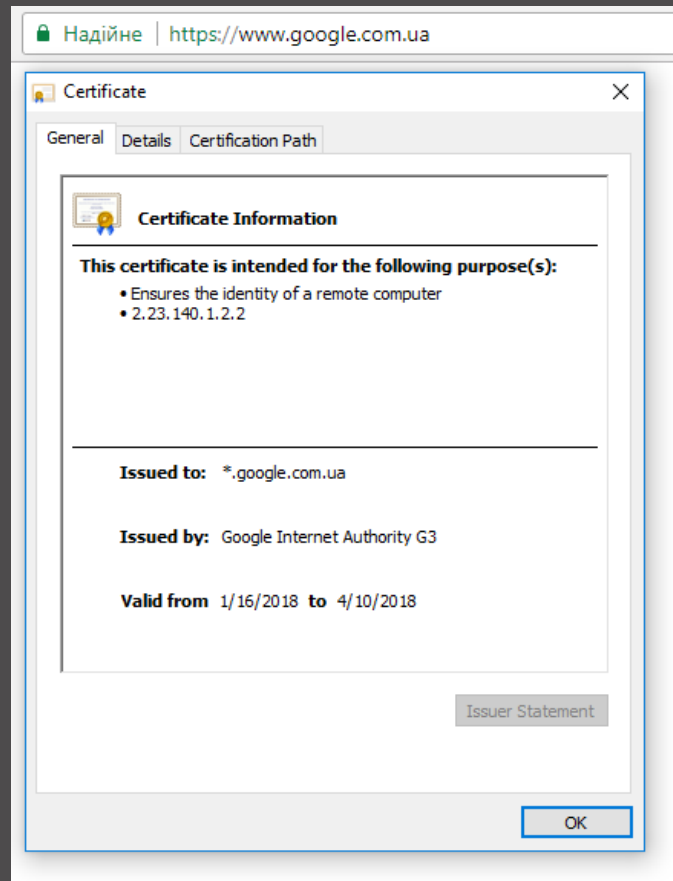


У цьому випадку пропонувалось увести дані, необхідні для аутентифікації на сторінці електронного банку



# Як не стати жертвою?

Перевіряти надійність ресурсу:



# Як не стати жертвою?

Перевіряти адреси посилань:

[www.google.com](http://www.google.com)

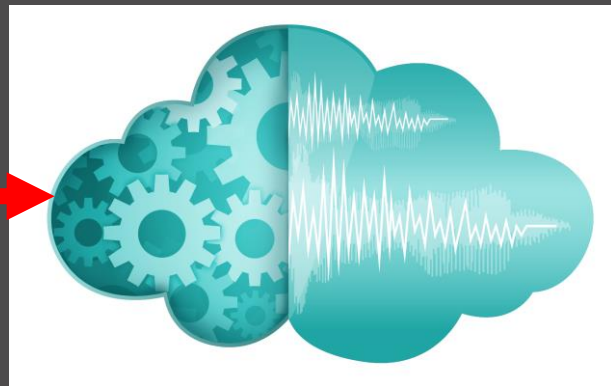
Посилання, отримане у листі  
або повідомленні

[www.g%D0%BE%D0%BEgle.com](http://www.g%D0%BE%D0%BEgle.com)

Посилання, після перевірки

# Як не стати жертвою?

За можливістю, не користуватися відкритими точками доступу до мережі «Інтернет» для виконання фінансових операцій чи авторизації у хмарних сервісах:



# Як не стати жертвою?

За можливістю, проводити підтвердження фінансових операцій та багаторівневої аутентифікації через пристрої, які працюють на стандарті **3G** та вище:



Дякую за увагу!



[www.cyberpolice.gov.ua](http://www.cyberpolice.gov.ua)

[facebook.com/cyberpoliceua](https://facebook.com/cyberpoliceua)

[twitter.com/cyberpoliceua](https://twitter.com/cyberpoliceua)