ONLINE FINANCIAL FRAUD

HOW CYBERCRIMINALS STEAL MONEY FROM USERS' BANK ACCOUNTS

Users are soft targets for financial cybercrime

Hacking banks is difficult – that's why criminals prefer to attack their customers

~ 1 900 000

users worldwide encountered banking malware attacks in 2013[1]

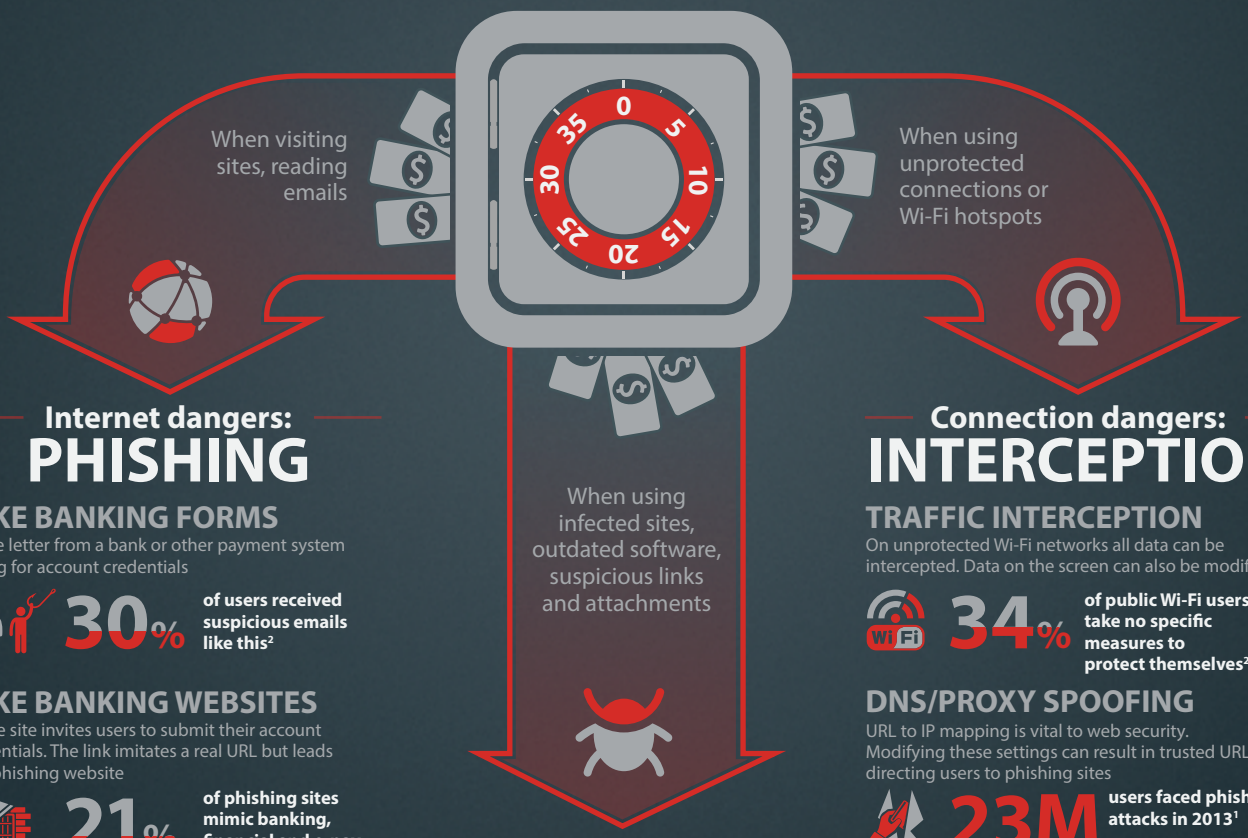
98% of users regularly access online financial services[2]

28% don't check website security when they enter confidential data[2]

38% carry out financial operations from mobiles and only 42% use mobile protection[2]

How can cybercriminals steal money from users?

Holders of online bank accounts can be targeted in a number of ways:



Internet dangers: PHISHING

FAKE BANKING FORMS

A fake letter from a bank or other payment system asking for account credentials

30% of users received suspicious emails like this[2]

FAKE BANKING WEBSITES

A fake site invites users to submit their account credentials. The link imitates a real URL but leads to a phishing website

21% of phishing sites mimic banking, financial and e-pay organizations[1]

Connection dangers: INTERCEPTION

TRAFFIC INTERCEPTION

On unprotected Wi-Fi networks all data can be intercepted. Data on the screen can also be modified

34% of public Wi-Fi users take no specific measures to protect themselves[2]

DNS/PROXY SPOOFING

URL to IP mapping is vital to web security. Modifying these settings can result in trusted URLs directing users to phishing sites

23M users faced phishing attacks in 2013[1]

Computer dangers: TROJANS

COLLECTING DATA WHEN IT'S ENTERED

Trojans intercept keystrokes or take screenshots, capturing sensitive info from regular or virtual keyboards. The Zbot Trojan is one of the most prominent examples.

8M attacks with Zbot were recorded by Kaspersky Lab in 2013[1]

USING WEB INJECTION

Trojans prompt users to enter data into rogue fields on legitimate pages. They can also imitate screens such as a list of user transactions or a simple "Blue screen"

$250M was stolen by cybercriminals using the Carberp Trojan in 2013[3]

BYPASSING TWO-FACTOR AUTHENTICATION

Many mobile Trojans work in tandem with their big brothers to intercept data from phones: Carberp-in-the-Mobile, Zeus-in-the-Mobile, etc.

268% more unique malware samples for Android OS were detected in 2013[1]

[1] Kaspersky Security Network [2] Consumer Security Risks Survey 2013, B2B International
[3] According to the Security Service of Ukraine

KASPERSKY