



Center for Career Development

by LINKgroup

How to defend ourselves against cyber-criminals - while home & at work -

22.05.2021 - Constantin-Cosmin Craciun

cosmin.craciun@cwavesoftware.com

Agenda

- Cyber-criminals – who are they?
- Types of cyber-crime acts
- Real world cases
- How can we defend ourselves
- Q&A

Cyber-criminals – who are they?

- People that take advantage of the technology (in different ways) in order to perform unlawful actions, aiming to gain a benefit (money, most often)
- The degree of tech usage and tech knowledge may vary
- Individuals or organizations, acting on their own or sponsored
- Too often called “hackers”



Cyber-criminals – what are they after?

Money

Reputation

Information

Pure
curiosity

Cyber-criminals – of all kinds

Script kiddies

Motivated individuals

Hacking groups

Organized criminal gangs

Nation states

Cyber-terrorists

Cyber-criminals – of all kinds

Identity thieves

Scammers

Phishers

Crackers

Hacktivists

Malware developers

Types of cyber-crime acts



Real world cases

1. The Romanian hacker "Guccifer"

Hacker Guccifer, who exposed Clinton private email server, ready for US prison sentence

Hacker was released on parole from Romanian prison this week and is now eligible for a second US extradition to serve 52 months in a US prison on a 2016 sentence.



THE UNITED STATES DEPARTMENT OF JUSTICE

ABOUT OUR AGENCY TOPICS NEWS RESOURCES CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE Thursday, September 1, 2016

Romanian Hacker "Guccifer" Sentenced to 52 Months in Prison for Computer Hacking Crimes

Marcel Lehel Lazar, 44, of Arad, Romania, a hacker who used the online moniker "Guccifer," was sentenced today to 52 months in prison for unauthorized access to a protected computer and aggravated identity theft.



AP NEWS

Top Stories Topics Videos Listen

Guccifer, Romanian hacker, extradited to U.S. to finish prison sentence: Reports

Andrew Blake The Washington Times November 13, 2016

BANK INFO SECURITY



REUTERS

World Business Markets Brea

Romanian Hacker 'Guccifer' Extradited to US

Former Taxi Driver Receives Conditional Release From Prison in Romania
Mathew J. Schwartz (@eurofobos) • November 15, 2016

INTERNET NEWS SEPTEMBER 1, 2016 / 7:30 PM / UPDATED 4 YEARS AGO

Romanian hacker 'Guccifer' sentenced to 52 months in U.S. prison

By Dustin Vois 2 MIN READ

WASHINGTON (Reuters) - A Romanian hacker nicknamed "Guccifer" who helped expose the existence of a private email domain Hillary Clinton used when she was U.S. secretary of state was sentenced on Thursday to 52 months in prison by a federal court in Alexandria, Virginia.



2. The “Anonymous” hacking group

The Return of Anonymous

The infamous hacker group reemerges from the shadows.

Story by Dale Beran

AT THE END OF MAY, as protests against the police killing of George Floyd **under way**, reports started to circulate that the shadowy hacker group Anonymous was back.



What actions have they taken?

Various forms of cyber-attack are being attributed to Anonymous in relation to the George Floyd protests.

First, the Minneapolis police department website was temporarily taken offline over the weekend in a suspected Distributed Denial of Service (DDoS) attack.

This is an unsophisticated but effective form of cyber-attack that floods a server with data until it can't keep up and stops working - in the same way that shopping websites can go offline when too many people flood it to snap up high-demand products.



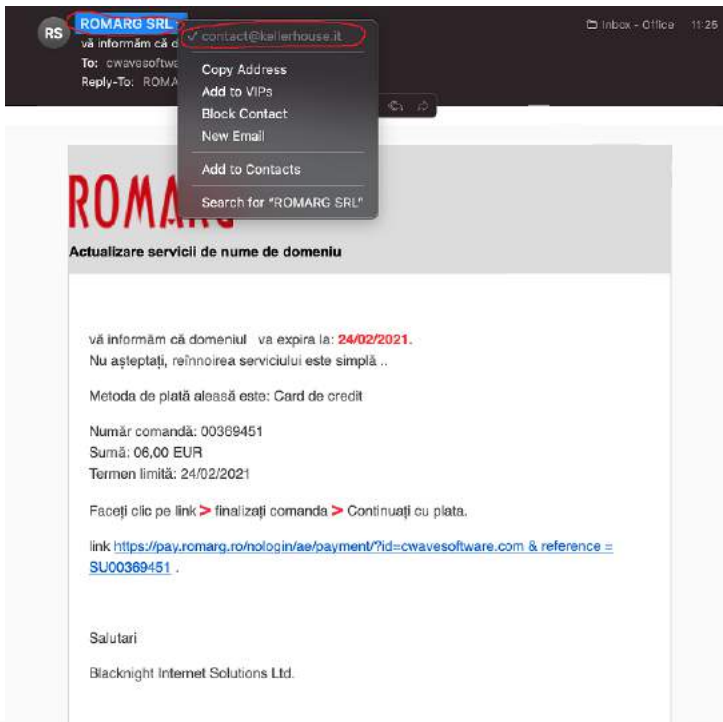
An emblem that is commonly associated with Anonymous. The “man without a head” represents **anonymity and leaderless organization**.^[1]



Individuals appearing in public as Anonymous, wearing Guy Fawkes masks

Motto	We Are Anonymous
Formation	c. 2004
Type	Multiple-use name/avatar Virtual community Voluntary association
Purpose	Anti-cyber-surveillance Anti-cyber-censorship Internet activism Internet vigilantism
Region served	Global
Membership	Decentralized affinity group

3. Phishing attempt 1



RS **ROMARG SRL** contact@kallierhouse.it Inbox - Office 11:25

vă informăm că d... va expira la: 24/02/2021.

To: cwavesoftware.com
Reply-To: ROMARG SRL

- Copy Address
- Add to VIPs
- Block Contact
- New Email
- Add to Contacts
- Search for "ROMARG SRL"

ROMARG

Actualizare servicii de nume de domeniu

vă informăm că domeniul va expira la: **24/02/2021**.
Nu așteptați, reînnoirea serviciului este simplă ..

Metoda de plată aleasă este: Card de credit

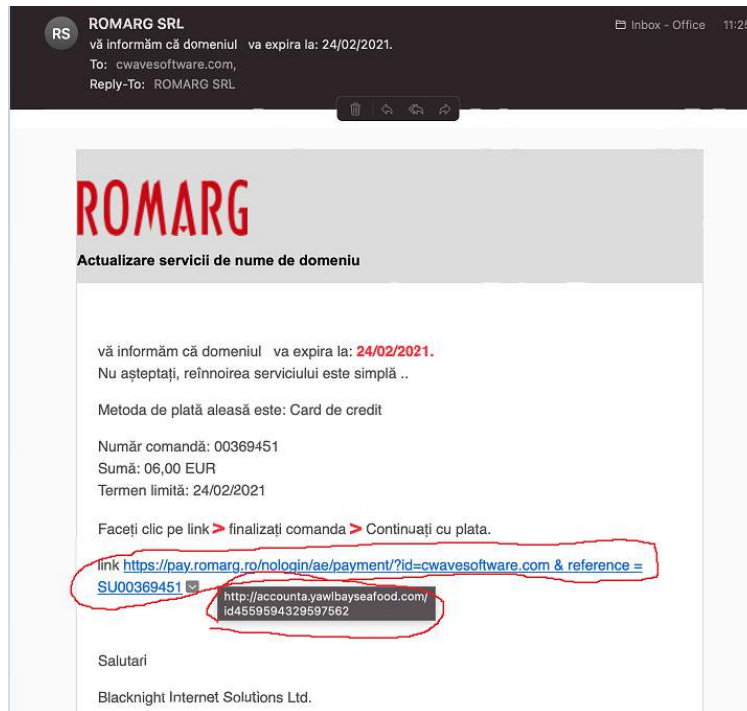
Număr comandă: 00369451
Sumă: 06,00 EUR
Termen limită: 24/02/2021

Faceți clic pe link > finalizați comanda > Continuați cu plata.

link <https://pay.romarg.ro/nologin/ae/payment/?id=cwavesoftware.com & reference = SU00369451> .

Salutari

Blacknight Internet Solutions Ltd.



RS **ROMARG SRL** Inbox - Office 11:25

vă informăm că domeniul va expira la: 24/02/2021.

To: cwavesoftware.com,
Reply-To: ROMARG SRL

ROMARG

Actualizare servicii de nume de domeniu

vă informăm că domeniul va expira la: **24/02/2021**.
Nu așteptați, reînnoirea serviciului este simplă ..

Metoda de plată aleasă este: Card de credit

Număr comandă: 00369451
Sumă: 06,00 EUR
Termen limită: 24/02/2021

Faceți clic pe link > finalizați comanda > Continuați cu plata.

link <https://pay.romarg.ro/nologin/ae/payment/?id=cwavesoftware.com & reference = SU00369451> .

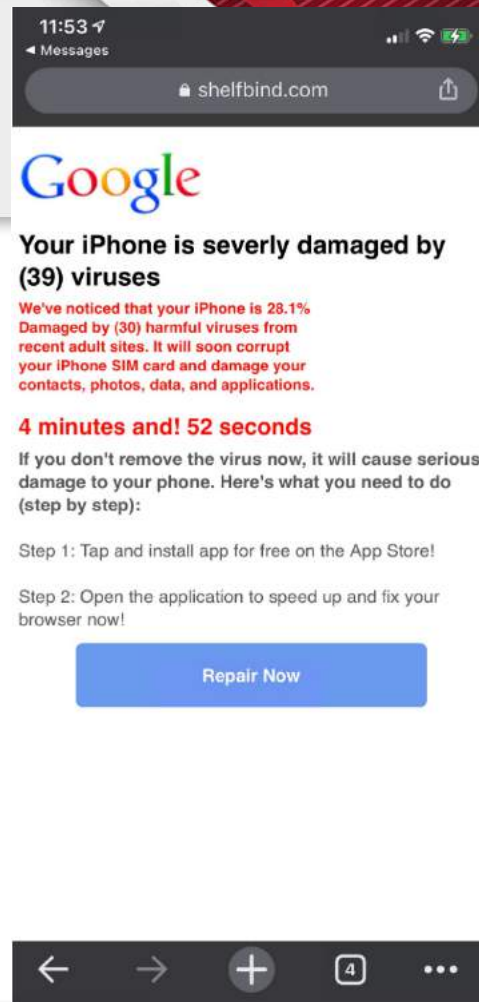
<http://account.yawlbyseafood.com/id4559594329597562>

Salutari

Blacknight Internet Solutions Ltd.



4. Phishing attempt 2



5. “The accident / COVID-19” scam



INSPECTORATUL DE POLIȚIE JUDEȚEAN BRAȘOV
BIROUL DE ANALIZĂ ȘI PREVENIRE A CRIMINALITĂȚII

PREVENIREA ÎNȘELĂCIUNILOR PRIN “METODA ACCIDENTUL”

Polițiștii brașoveni au informat cetățenii de nenumărate ori asupra riscurilor la care se supun dacă dau crezare anumitor persoane care, prin diferite metode, încearcă să obțină de la ei diverse sume de bani.

Acțiunea infracțională în cazul “Metodei Accidentul” constă în realizarea contactului telefonic cu victima, căreia i se comunică o știre șocantă, în esență constând în aceea că **un membru al familiei sale a fost implicat într-un accident rutier care s-a soldat cu urmări grave, iar pentru diminuarea consecințelor legale și/ sau medicale ale evenimentului se solicită o sumă importantă de bani.**



POLITICĂ ACTUALITATE ECONOMIE EXTERNE SPORT TV MAGAZIN MAI MULTE

HOME > Știri > Actualitate > Evenimente > „Metoda Accidentul” devine „metoda COVID”: Cum a reușit o grupare să obțină 100.000 de lei

„Metoda Accidentul” devine „metoda COVID”. Cum a reușit o grupare să obțină 100.000 de lei

6. The “Nigerian Prince” scam

Internal Memo:

146 Hagley Road, Birmingham
Birmingham B3 3PJ

From the Desk of
Mr. Jerry Smith
Date: 13/01/14

Attn: Sir/Madam,

I seize this opportunity to extend my unalloyed compliments of the new season to you and your family hoping that this year will bring more joy, happiness and prosperity into your household.

I am certain that by the time you read this letter I might have already gone back to my country **United Kingdom**. I visited South Africa during the New Year period and during my stay, I used the opportunity to send you this letter believing that it will reach you in good state.

My name is **Mr. Jerry Smith**, I am the auditor and head of computing department of a bank here in United Kingdom. I wish to inform you of a bank account that was opened in our bank since my inception into office in **2001**, and according to our record, it was evident that nobody has ever operated on this account since then. I therefore took the courage to look for a reliable and honest person who will be capable for this important transaction.

The owner of this money is **Late Mr. Mutassim Biliah Gaddafi**, the son of **Late Muammar Gadafi of Libya**; He was captured by anti-Gadafi forces later killed alongside with his father. No other person knows about this money or anything concerning his account and the account has no next of kin and my investigation further proved to me that his family and his country does not know anything about this account.

I am therefore seeking for a reliable person that will play the human role as the next of kin to this fund which is in the amount of **£32,000,000.00 (Thirty Two Million Pounds Sterling)**. I have also discovered that if I do not remit this money out urgently, it will be forfeited to the government treasury account as an unclaimed fund.

Please respond immediately via my private email address: jjerrysmith@aol.com

I will use my position and influence to effect the legal approval and onward transfer of this fund into any nominated bank account of your choice with appropriate clearance from foreign payment department.

You will henceforth stand to get 35% while 5% shall be set aside for the expense that will be incurred during the process, and 60% will be for me.

I will fill you in with further details upon your swift reply. Please be informed that confidentiality of this transaction is of utmost importance.

Yours Truly,



Mr. Jerry Smith.



7. SIM swap identity theft



VIDEO Percheziții la hackerii vedetelor. Metoda prin care au fost lăsați fără bani în cont maneliști și cântăreți cunoscuți

VIDEO Furt de identitate pornit de la telefonul mobil / Cel puțin 50 de oameni au rămas fără banii din conturi

de I.H. HotNews.ro
Miercuri, 18 noiembrie 2020, 11:20 Actualitate | Esențial

O grupare a reușit să acceseze conturile bancare a cel puțin 50 de persoane, creând un prejudiciu de peste 100.000 de lei, după ce a obținut datele acestora prin substituirea cartelelor SIM ale telefoanelor mobile. De asemenea, ar fi postat pe paginile de socializare ale victimelor sau ar fi transmis mesaje private persoanelor din listele de prieteni, solicitând transferuri de bani.



SECURITATEA INFORMATIEI

INFORMATIA ESTE VALOARE SI TREBUIE PROTEJATA!

HOME OFERTA STIRI



SIM SWAP – FRAUDĂ PRIN INTERMEDIUL ÎNLOCUIRII CARTEI SIM

IN: GDPR - LEGISLATIE - SECURITATE IT - ALERTE DE SECURITATE - NOUATI, INGINERIE SOCIALA, SECURITATEA INFORMATIEI

Peste 50 de persoane au fost victimele unei metode noi de furt de identitate. O grupare monitorizată de luni de zile prelua controlul asupra numărului de telefon al victimei, invocând la companiile de telefonie mobilă fie defectarea cartei SIM, fie pierderea telefonului. Odată intrați în posesia numărului de telefon al victimei, preluau controlul asupra conturilor de pe rețelele de socializare, dar și asupra conturilor bancare. Fără măcar să își dea seama, oamenii rămăneau fără bani în conturi sau rudelor și cunoscuților li se cereau sume mari de bani împrumut.





8. Advanced Persistent Threats

APT41

Suspected attribution: China

Target sectors: APT41 has directly targeted organizations in at least 14 countries dating back to as early as 2012. The group's espionage campaigns have targeted healthcare, telecoms, and the high-tech sector, and have historically included stealing intellectual property. Their cyber crime intrusions are most apparent among video game industry targeting, including the manipulation of virtual currencies, and attempted deployment of ransomware. APT41 operations against higher education, travel services, and news/media firms provide some indication that the group also tracks individuals and conducts surveillance.

Overview: APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Associated malware: APT41 has been observed using at least 46 different code families and tools.

APT39

Suspected attribution: Iran

Target sectors: While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry.

Overview: The group's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making.



APT38

Suspected attribution: North Korea

Target sectors: Financial institutions world-wide

Overview: Our analysis of the North Korean regime-backed threat group we are calling APT38 reveals that they are responsible for conducting the largest observed cyber heists. Although APT38 shares malware development resources and North Korean state sponsorship with a group referred to by the security community as "Lazarus", we believe that APT38's financial motivation, unique toolset, and tactics, techniques, and procedures (TTPs) are distinct enough for them to be tracked separately from other North Korean cyber activity.



9. Ransomware computer virus

Take a look at the history of ransomware, the most damaging ransomware attacks, and the future for this threat.

Ransomware has been a prominent threat to enterprises, SMBs, and individuals alike since the mid-2000s. In 2017, the FBI's Internet Crime Complaint Center (IC3) received [1,783 ransomware complaints that cost victims over \\$2.3 million](#). Those complaints, however, represent only the attacks reported to IC3. The actual number of ransomware attacks and costs are much higher. In fact, there were an estimated [184 million ransomware attacks](#) last year alone. Ransomware was originally intended to target individuals, who still comprise the majority of attacks today.

CASE STUDY: RANSOMWARE ATTACK COSTS BUSINESS \$1 MILLION+

Recently, a mid-size manufacturing company (that has asked to remain nameless, for obvious reasons) was hit with a ransomware attack that cost them more than a million dollars - but the good news is it will never happen again, thanks to our technology integration with IT services provider Xenium.





What do those examples have in common?





Don't take as granted all that you see in the news



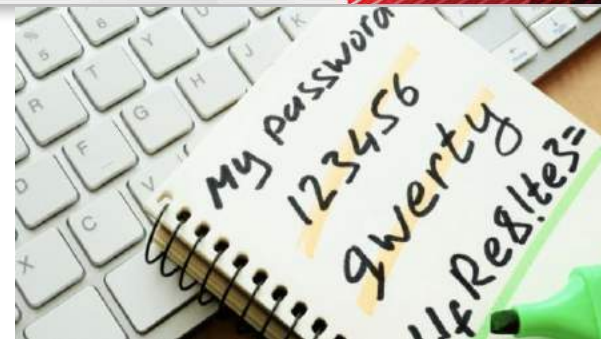


What can we do about it?

<https://www.youtube.com/watch?v=u8qgehH3kEQ>

1. Protect your accounts

- Use strong passwords: long enough, hard to guess, Lowercase + uppercase + numeric + special characters
- Do not use same password for more than one account
- Do not write your password down on physical support. Use password management software instead
- Enable 2FA where possible
- Pay attention what password recovery mechanism you choose
- Pay attention what personal information you share



<https://www.youtube.com/watch?v=opRMrEfAlil>



Center for Career Development

by LINKgroup

Password	Number of users	Time to crack it	Times exposed
123456	2,543,285	Less than a second	23,597,311
123456789	961,435	Less than a second	7,870,694
picture1	371,612	3 Hours	11,190
password	360,467	Less than a second	3,759,315
12345678	322,187	Less than a second	2,944,615
111111	230,507	Less than a second	3,124,368
123123	189,327	Less than a second	2,238,694
12345	188,268	Less than a second	2,389,787
1234567890	171,724	Less than a second	2,264,884
senha	167,728	10 Seconds	8,213
1234567	165,909	Less than a second	2,516,606

2. Ignore suspicious emails / messages

- messages containing weird sentences, grammar or spelling mistakes
- messages asking you to claim any prizes
- messages that warns you about loosing your account if you don't follow the instructions
- etc.

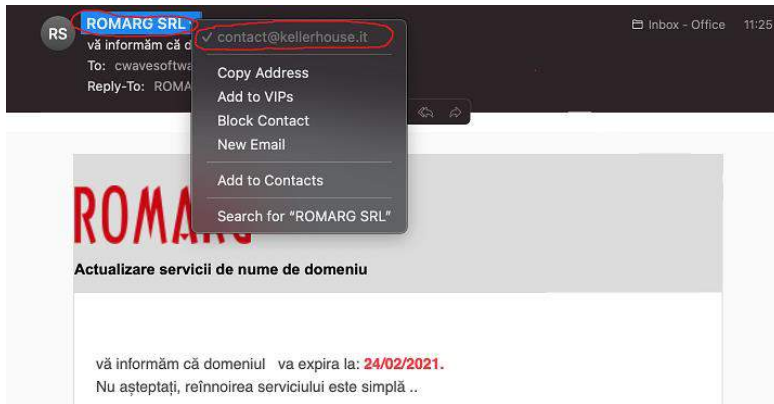
**Do not
reply**

**Do not open
files**

Do not click



2. Ignore suspicious emails / messages – additional checks


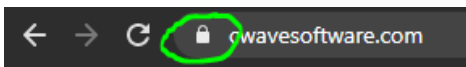


Do not
reply

Do not open
files

Do not click


3. Stop ignoring warnings



Your connection is not private

Attackers might be trying to steal your information from **esxi.cwavesoftware.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

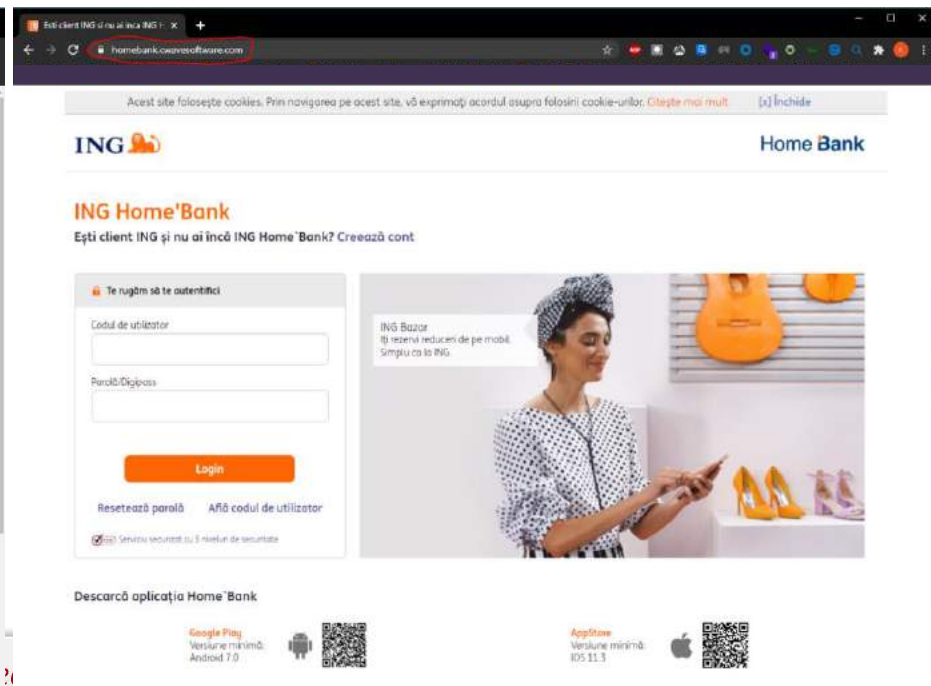
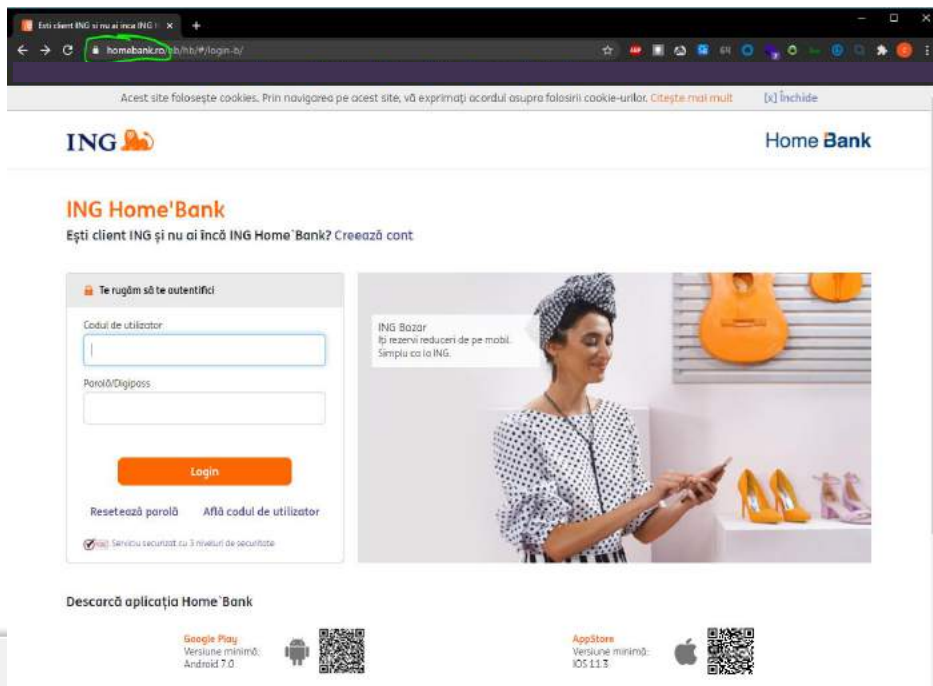
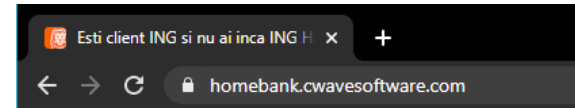
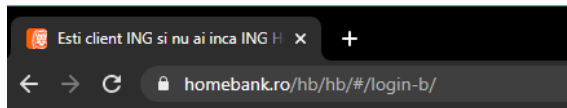
 To get Chrome's highest level of security, [turn on enhanced protection](#)

[Hide advanced](#) [Back to safety](#)

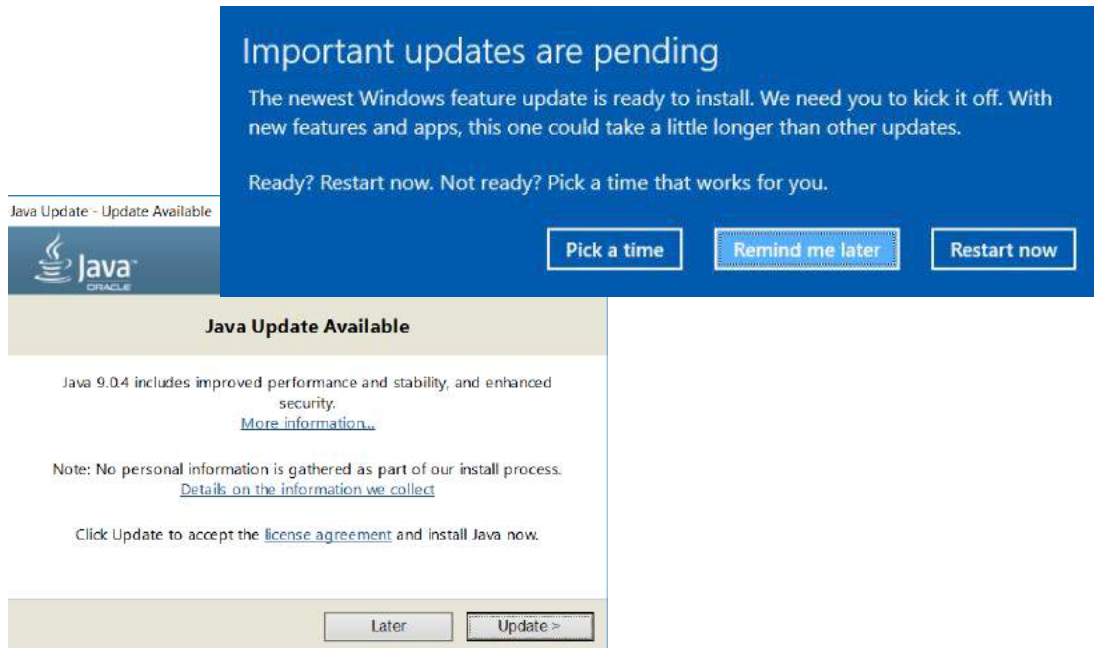
This server could not prove that it is **esxi.cwavesoftware.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

~~[Proceed to esxi.cwavesoftware.com \(unsafe\)](#)~~

4. Pay attention to URLs



4. Keep your software and antivirus up to date




Important updates are pending

The newest Windows feature update is ready to install. We need you to kick it off. With new features and apps, this one could take a little longer than other updates.

Ready? Restart now. Not ready? Pick a time that works for you.

Java Update - Update Available

 **Java**
ORACLE

Java Update Available

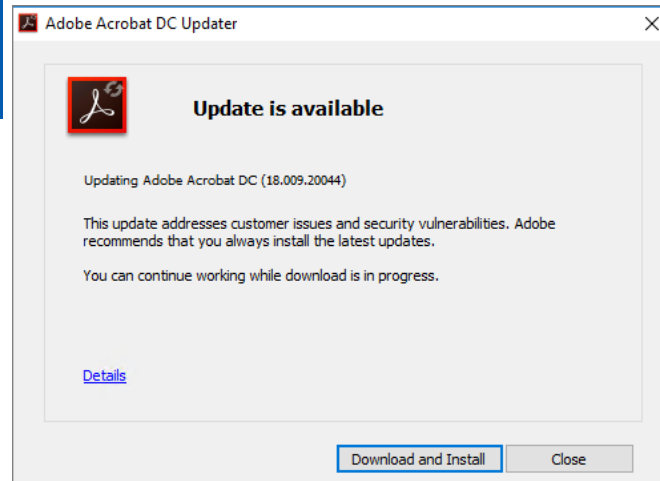
Java 9.0.4 includes improved performance and stability, and enhanced security.
[More information...](#)

Note: No personal information is gathered as part of our install process.
[Details on the information we collect](#)


Click Update to accept the [license agreement](#) and install Java now.

Later Update >

Pick a time Remind me later Restart now



Adobe Acrobat DC Updater

 **Update is available**

Updating Adobe Acrobat DC (18.009.20044)

This update addresses customer issues and security vulnerabilities. Adobe recommends that you always install the latest updates.

You can continue working while download is in progress.

[Details](#)

Download and Install Close

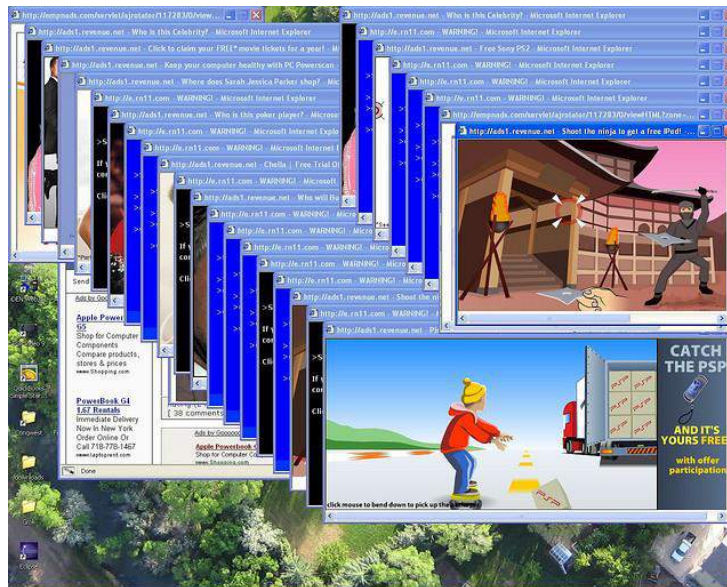


5. Stop using pirated software





6. Spot any unusual behavior of your computer / smartphone / tablet



7. Don't be fooled





8. Ask your friends and family to do all of the above



What should I do if ...



<https://cert.ro/contact>

	At home	At work
I get a suspicious email	Ignore	Notify IT/IS dept.
My computer is infected	Inform authorities	Notify IT/IS dept.
I get a suspicious phone call	Inform authorities	Inform authorities/ IT/IS dept.
My computer is acting weird	Ask an expert to take a look	Notify IT/IS dept.
I accidentally visit a suspicious website	Leave that website	Leave that website
My account is compromised	Recover and change your password (if it's not too late). Make sure you don't use the old password for any other account	Notify IT/IS dept.



Center for Career Development by LINKgroup

office@dezvoltarea-carieriei.com

www.dezvoltarea-carieriei.com

+40 (314) 336 211

LINK Academy™

Școală pentru o carieră IT profitabilă

office@link-academy.com

www.link-academy.com

Înscrieri: +40 (314) 326 162

+40 (314) 326 163

Adresa: Academiei Center, Strada Academiei nr. 39-41, Etaj 2, Sector 1, București

Business Academy™ by LINKgroup

Școala oamenilor de afaceri

office@business-academy.ro

www.business-academy.ro