



Funded by the
Erasmus+ Programme
of the European Union

Cyber-Attacks: Social Engineering and Phishing

Social Engineering Modules and Manipulation

Safeguarding against Phishing in the age of 4th Industrial Revolution

www.cyberphish.eu

This project has been funded with support from the European Commission.

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.



Learning Goals

Explain different types of Phishing attacks and learn to recognise them

Phishing attacks:

- Event-based attacks, Emails, Instant Messaging, Social networks, Websites, Lotteries scams, SMS, Phone calls, Face to face, Shoulder surfing.

Combination of techniques:

- Spray and Pray, Spear Phishing, Whaling, Vishing, Smishing, Angler Phishing, Clone Phishing, Malvertising.

Student Workload



Lecture	4 h
Audio and video material	2 h
Case studies	2 h
Further reading	2 h
Preparation for exam	2 h



Scams via Emails
Fake Wins

Shoulder Surfing

Fake Surveys

Scams via SMS

Baiting

Fake Websites

Scams in Social Media

Vishing

Tailgating

Scams via Instant messaging



Phone calls

SMS

Emails

**Come inside
organisation**

Results of Successful Phishing Attack

- loss of sensitive data
- loss of credentials (usernames and passwords)
- Identity theft
- Theft of client information
- loss of funds from business and client accounts
- Access to IS to launch future attacks
- Unauthorized transactions
- loss of intellectual property
- Data provided or sold to criminal third parties
- Disruption of operational activities
- Incident response
- Eradication and recovery
- lost working hours for recovery
- Reputation damage
- loss of income
- Fines, legal fees
- ...

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Events-based Attacks

- Large scale events, wars, pandemics, like COVID-19, cause people to act more impulsively than they would under normal circumstances
- The most used techniques: emails, spear phishing, SMS, tailgating, vishing etc.

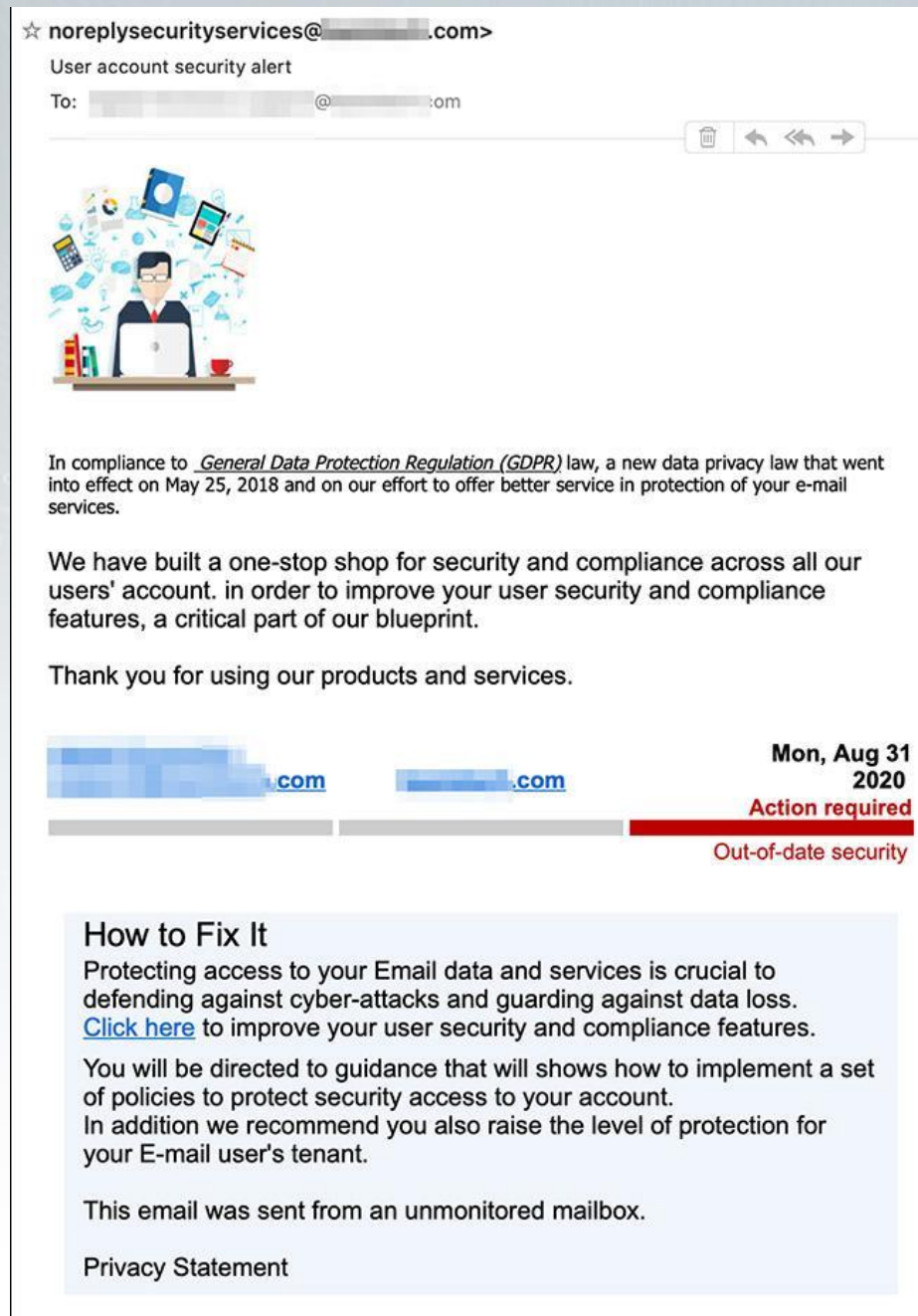
GDPR Related Attacks

- **General Data Protection Regulation (GDPR)** is a Regulation, which, on data protection and privacy in European Union GDPR, which valid since 2018, controls companies and organisations handle personal data
- Companies conducting automated or partially automated processing of personal data must follow GDPR
- Many GDPR attacks occurred in 2018, as all companies and organisations must implement GDPR in their organisations

GDPR Related Attack to Organizations

- **Why this type of attachment is successful?**
Companies did not have enough knowledge about GDPR.
- **Target:** organisations employees, usually to
 - company emails that are available on the internet or
 - direct to executives or upper managers of companies (which hopefully has access to client data or are responsible for GDPR compliance)
- **Threat:** emails from “security organisations” providing services to improve user security and compliance to GDPR
- **Attack method:** emails (spear phishing).
- **Phishing tactic:** emails designed and formatted look legitimate. Attackers created impression that emails were originated from a legitimate source
- **Phishing factor:**
 - **fear about law violations**
 - **Inspiring sense of urgency:** attackers used timeline for supposed GDPR compliance that was regularly updated by the attackers to increase the pressure on the recipient
- **Vulnerabilities:**
 - Not trained personal (which clicks on the link in the email and provides data)

GDPR related attack: improving user security and compliance to GDPR



- Phishing website will be opened, when victim clicks on the link
- Website could be personalized with victims' email address
- Victim could be asked to login to (providing login data) the fake website, which looks like real website
- **Result:**
 - Stolen victims' email login data to get access to email
 - Sensitive data could be stolen from victim' email or stolen contacts could be used for further cyberattacks

GDPR Related Attack to Clients

- **Why this type of attachment is successful?**
Companies sent emails to clients regarding GDPR updates regarding clients' data privacy policies.
- **Target:** clients of various organisations, usually IT services providers, financial organisations' clients
- **Threat:** emails from “organizations” asking to confirm permission to store and process personal data
- **Attack method:** emails.
- **Phishing tactic:**
 - emails designed and formatted look like real organisation email. Attackers created impression that emails were originated from a legitimate source.
 - attackers use trusted brands
- **Phishing factor:**
 - **Commitment and consistency**
 - **Loyalty to the organization**
- **Vulnerabilities:**
 - Clients with limited or any knowledge about phishing (which clicks on the link in the email and provides data)

GDPR Related Attack: Accept New Privacy Policy



- Phishing website will be opened, when victim clicks on the link
- Victim could be asked to provide their personal information, including account credentials and payment card information to the fake website, which looks like real website.
- **Result:**
 - stolen Victims' email login data to get access to email. Sensitive data could be stolen from victim' email or stolen contacts could be used for further cyber attacks.
 - Stolen financial data.
 - Infected devices (i.e., keyloggers, ransomware etc.)

Source: <https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/>, Redscan

COVID Related Attacks

- During COVID-19 pandemic many people were working from home. Employees used their personal computers for performing job tasks in remote mode, basic communication was via emails – this means that employees became more vulnerable to cyberattacks
- During COVID-19 was noticed an uptick on pandemic-related scams, like fake Centers of Disease Control and Prevention (CDC) or health organizations' emails, emails about vaccine coverage, where you can get vaccine, vaccine statistics, status of employees' vaccination etc.

Covid Attacks: Emails

- **Why this type of attachment is successful?** COVID-19 caused people a sense of instability and uncertainty, frequent politicians' decisions changes regarding quarantine, vaccination, proof documents about vaccination etc.
- **Target:** all citizens
- **Threat:**
 - emails asking to provide sensitive information on fake website
 - emails asking to click on a link
- **Attack method:** emails.
- **Phishing tactic:**
 - emails designed and formatted look like real organisation email
 - attackers usually suggest to download document to review COVID-19 statistics, download covid form, fill in online form or fill in downloaded documents about vaccination status, upload negative test etc.
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **Asks to follow non-standard process**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing (citizens which perform actions asked in the phishing emails)

Covid Attacks: Health Advice Email



- Phishing website will be opened, when victim clicks on the link, which looks like a link to PDF file
- Victim could be asked to provide their personal information, including account credentials and payment card information in order to “authenticate identity” to the fake website.
- **Result:**
 - Stolen victims’ email login data to get access to the email.
 - Stolen financial data.
 - Infected devices (i.e., keyloggers, ransomware etc.)

Covid Attacks: SMS

- **Why this type of attachment is successful?**

COVID-19 caused people a sense of instability and uncertainty, frequent politicians' decisions changes regarding quarantine, vaccination, proof documents about vaccination etc. Large scale events, wars, pandemics, like COVID-19, cause people to act more impulsively than they would under normal circumstances.

- **Target:** all citizens

- **Threat:**

- emails asking to provide sensitive information on fake website
- emails asking to click on a link

- **Attack method:** SMS.

- **Phishing tactic:**

- emails designed and formatted look like real organisation email
- attackers usually suggest to download document to review COVID-19 statistics, download covid form, fill in online form or fill in downloaded documents about vaccination status, upload negative test etc.

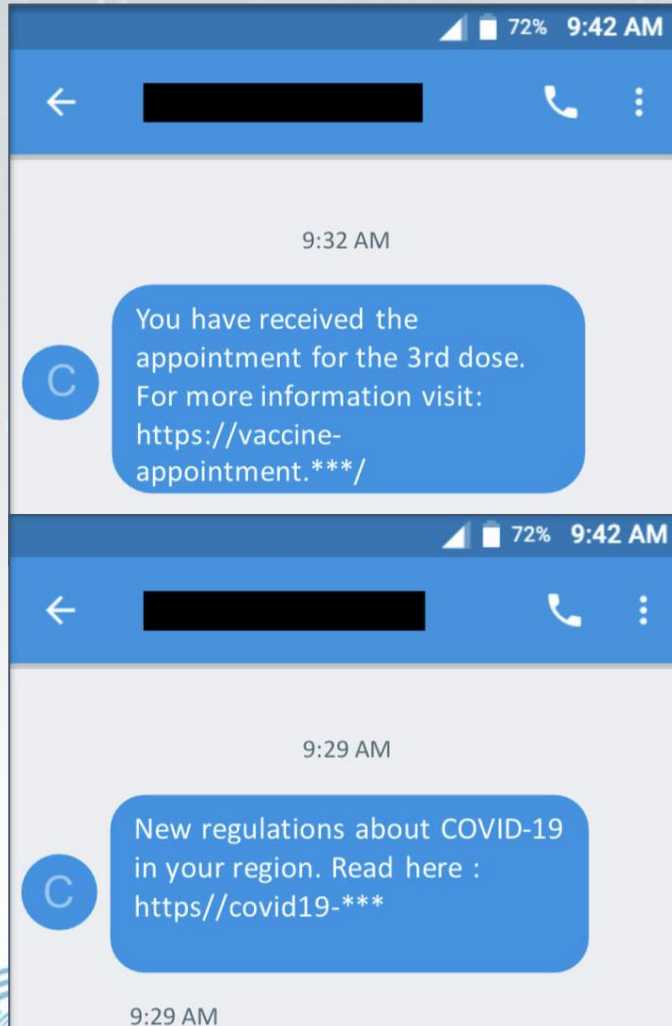
- **Phishing factor:**

- **Inspiring sense of urgency**
- **Inspiring sense of scare**
- **Asks to follow non-standard process**

- **Vulnerabilities:**

- citizens with limited or any knowledge about phishing (citizens which perform actions asked in the phishing emails)

Covid Attacks: Information About Vaccines via SMS



- **Why this type of attachment is successful?** Institutions send SMS's to citizens regarding vaccination.
- **Target:** all citizens
- **Threat:**
 - SMS's asking to click the provided link
- **Attack method:** SMS.
- **Phishing tactic:**
 - SMS are short. One or two sentences. A link to the fake website usually is provided in the SMS
- **Phishing factor:**
 - sense of instability and uncertainty
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing (citizens which perform actions asked in the phishing emails)

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Phishing emails

- One of the most well-known phishing types
- Attackers could use such tactics in the phishing emails:
 - Requests to send sensitive information via email
 - Asks to click provided link in the email
 - Asks to open attachment, usually in PDF or DOC formats
- Usual topics of phishing emails:
 - Account problems
 - Tech support issues
 - Romantic relationship
 - Spear phishing emails for CEOs and managers
 - To recover, reimburse money or to get financial support from institution

Phishing Emails

You could face several terms related to phishing emails:

- **Spray and pray** – malicious emails that are sent to any email addresses in an attempt to steal sensitive information
- **Advanced fee scam** – common fraud associated with nationals from Nigeria, e.g., asking for assistance in moving a large amount of money
- **Spear phishing** – malicious emails that are specially crafted and sent to a specific individual or organisation in an attempt to steal sensitive information
- **Whaling** – an attempt to steal sensitive information and is often targeted at senior management
- **Angler Phishing** – a relatively new type which refers to attacks that exist on social media using fake URLs, cloned websites, posts, and tweets as well as instant messaging
- **Clone Phishing** – a type of phishing where a legitimate and previously delivered email is used to create an identical email with malicious content
- **Malvertising** – this phishing type uses online advertisements or pop-ups to compel people to click a valid-looking link that then installs malware on their computer

Phishing Emails: Requests to Send Sensitive Information via Email

- **Why this type of attack is successful?** Phishing attacks look convincing with impression as a trusted source. Organisations are not performing sufficient due diligence. Attackers use more sophisticated phishing attacks, which difficult to detect etc.
- **Target:** all citizens
- **Threat:**
 - emails asking to send response
 - emails asking to provide sensitive information via email
- **Phishing tactic:**
 - looks for partners, has good news to victim, offers money, informs about winning, someone pretends as a friend and ask to loan money because of unexpected disaster etc.
 - offers money, informs about contest winner etc.
- **Phishing factor:**
 - **Gives the impression to victim that the sender is useful**
 - **Instils greediness**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing (citizens which reply or perform actions asked in the phishing emails)
- **Result:**
 - Identity theft, loss of money

Examples of Phishing Emails: Requests to Send Sensitive Information via Email

Sender: eduardorodriguez <andreasjohnson874@gmail.com>

To: andreasjohnson847@gmail.com

Subject:

Hello My Friend

I am ANTONI FELIKS from Poland, I have a good news for you
CONGRATULATIONS!!!

Contact me now on this email: homebankpln@gmail.com or
homebankpln@polandmail.com to receive a good news

Sender: administrator <admin@www-professionals.online>

To:

Subject: Congratulations!!!

We are pleased to inform you that your email has won \$ 7,500
from www online lottery award. In order to get this award you are
required to provide such information:

Beneficiary name and surname: _____

Beneficiary address: _____

Beneficiary country: _____

Beneficiary credit card number: _____

Beneficiary credit card CVC2: _____

NOTE: keep your winning information confidential.

Signed

CEO: Luis Andres Jonson

Sender: Ava Williams <avawilliamsj@gmail.com>

To: avawilliamsj@gmail.com

Subject: Hi...

Greetings to you

I know that you will be surprised to receive this message from me because we have not met before. I
got your email from Google research. I am writing to you from a hospital where I have been undergoing
medical treatment because I am very sick now as a result of cancer.

I contacted you today because I need your help to invest the funds I inherited from my late husband.
I will compensate you with 30% of the money if you agree to help me with this.
I will tell you more about myself and my plans when I hear back from you.

Regards

Mrs. Ava Williams

Sender: manyrib7@gmail.com

To:

Subject: Hi...

My name is Rihab Manyang, I am here to find a business partner
or friend to help me invest my fund in your country.



Phishing Emails: Asks to Click Provided Link in Email

- **Why this type of attackment is successful?** Phishing attacks looks convincing with impression as a trusted source. Organisations are not performing sufficient due diligence. Attackers use more sophisticated phishing attacks, which difficult to detect: they can use combination of content, context and emotional motivators what drives the success of a phishing attack etc.
- **Target:** all citizens
- **Threat:**
 - phishing attacks copy our existing workflows
 - attackers ask to click provided link in the email
- **Phishing tactic:**
 - Emails regarding compromised email addresses or passwords
 - Emails regarding shared documents for collaboration
 - Emails informing about technical problems
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **Attackers preys on emotions and instincts of the victim**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing (citizens which reply or perform actions asked in the phishing emails)
- **Result:**
 - Identity theft, loss of money

Main Features of Phishing Emails

- Use reputable organisations or persons names
- Use data of reputable sources
- Ask to provide sensitive information
- Emails could have attachments
- Usually unknown recipient
- Links to websites (links could be shortened)
- The links traditionally go to malicious websites
- Use fear or convey sense of urgency
- Implausible pretext to be true (lottery, discounts, inheritance,...)

Links Used in Phishing Emails

- Attackers in the phishing emails usually use links to fake websites:
 - Attackers could register fake domain. URL name could be similar to real organization, they just change one or several letters in the domain name, like instead of letter “l”, they can use letter “i”, or instead of “m”, use “rn” etc. For example, they could register such fake domain name www.exarnple.com (real URL www.example.com)
 - Attackers could register domain by using real organization name in the URL, like, www.sales-organization.com (real URL www.organization.com)
 - Attackers could use shortened URLs, like Bitly, TinyURL, Short.io (more information in the [section shortening services](#))
 - Attackers could use the link of hacked website (by using real domain name, but another part of URL is created by hackers)
 - Attackers includes malicious code in legitimate webpage (Injection attack). When victim open this website malicious script will be executed. The result of such type attack would be data theft, keylogging, cookie theft etc.

Sender: NB Online Fraud Prevention <info@nat1onalbank.com>



To: undisclosed-recipients

Subject: Your National Bank account has been suspended



Dear Customer,

We recently noticed that different devices from different locations tried to login to your National Bank account.

We provide the list of IP addresses with recent attempt to login to your account :

12.55.155.6:8080

32.44.789.99:3128

54.22.124.44:8080

78.44.457.14:80

Currently your account is SUSPENDED. You need to activate it within 7 days, otherwise account will be blocked.

To confirm that you are original user and activate account, please click [HTTP://WWW.NAT1ONALBANK.COM?PROFILE](http://www.nat1onalbank.com/?PROFILE)

More information [here](#).

<http://www.nat1onalbank.com/?PROFILE>

Sincerely,

National Bank Online Fraud Prevention Manager

JohnBank@gmail.com



Report-of-attempts-to-login.zip

Phishing Emails with attachment or File Download

- **Why this type of attachment is successful?** Phishing attacks look convincing with impression as a trusted source. Organisations are not performing sufficient due diligence. Attackers use more sophisticated phishing attacks, which are difficult to detect: they can use a combination of content, context and emotional motivators that drive the success of a phishing attack etc.
- **Target:** all citizens
- **Threat:**
 - phishing attacks copy our existing workflows
 - attackers ask to open attachment pictures, music, movie, documents (like PDF, DOC, ZIP) that have malicious software embedded
 - attackers attach HTML files, which are fully functional – they have all elements that are needed for phishing, attackers do not need to publish on the internet
- **Phishing tactic:**
 - Emails with attachments: file with business or individual proposal, file with “confidential” or “very important” information, sales or financial (unpaid invoices, purchase order) information, urgent voice email, updated organisational policy, files with technical problems, time-specific information, like pandemic etc.
 - Emails asking to fill in attachment document for important workflows
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Attackers prey on emotions and instincts of the victim**
- **Vulnerabilities:**
 - users with limited or any knowledge about phishing (citizens who open attachment)
- **Result:**
 - Infected computers, identity theft, loss of money

Examples of Phishing Emails: Phishing Emails with attachment or File Download

Do not trust links and attachments in the email, even if it is from a trusted person

Sender: Jaana Jordan<cdg446@comcast.net>

To: Una Vilime <una.vilime@organisationname.com>

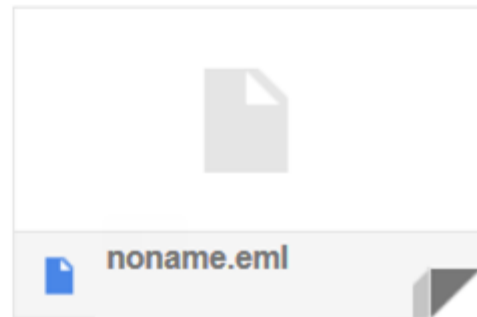
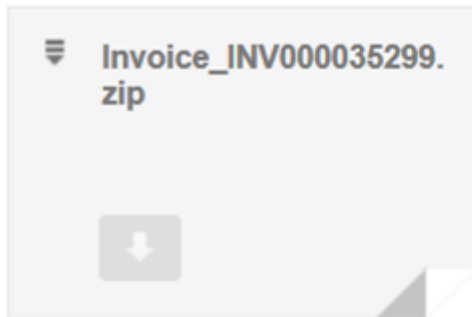
Subject: hi Una

You need to process a Faster payment for an invoice urgently, kindly let me know if you are available asap.

Regards

Jaana Jordan

Sent from my iPhone



Sender: ABC Bank<noreply@support-abcbank.com>

To:

Subject: ABC bank Account Support Department

Dear ABC Bank user,

We noticed unusual activity in your credit/debit account. As a result we have to limit access to your bank account. Your limited access will remain until the issue has been resolved.

We work to ensure your account safety, therefore we appreciate your understanding.

In order to ensure your safety we attach a document which you need to open in a web browser. Follow provided steps in the opened web page to restore your account.

Sincerely

ABC bank Account Support Department



Account-Update.html

Examples of Phishing Emails: Phishing Emails with attachment or File Download

Sender: WeTransfer <noreply@wetransferring-files.net>

To: me

Subject: info@wetransferring-files.net sent you policy.doc via WeTransfer



info@wetransferring-files.net sent you policy.doc via WeTransfer

1 item, 25.6 KB in total ▪ Expires after 2 days

Important information for staff!

Please find attachment confidential file - updated organisational policy. Please download it and read it carefully, otherwise you won't be able to access your workplace premises or information systems. System Security Team

[Get your file](#)

Download link <https://bit.ly/2YI6BY6>

Sender: Microsoft Security Team <support@dig-support.com>

To:

Subject: Important: data security alert



Dear Microsoft User,

Taking care of your online safety, we send you a safety message. We noticed that your document with sensitive data is freely available on the Internet.

We remind you that by sharing sensitive information of other people, you are in breach of GDPR. This could result in a hefty fine.

Please download the document and change sharing options.

[Download document.](#)

Microsoft Security Team

Spear Phishing

- **Why this type of attack is successful?** Spear phishing messages target each intended victim, spear phishing attacks happen over time, spear phishing leverages zero-day exploits, companies lack or don't enforce computer use policies, each spear phishing email looks authentic, Victim complies with request etc..
- **Target:** employees: Chiefs of Staff to the C-team, accountant team, HR team, payroll team etc.
- **Threat:**
 - phishing attacks copy our existing workflows
- **Phishing tactic:**
 - Emails with attachments: file with business or individual proposal, file with "confidential" or "very important" information, sales or financial (unpaid invoices, purchase order) information, urgent voice email etc.
 - Emails with links to fake website
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Attackers preys on emotions and instincts of the victim**
- **Vulnerabilities:**
 - employees with limited or any knowledge about phishing
- **Result:**
 - loss of confidential information, loss of intellectual property, loss of business secrets, infected digital devices etc.

Example of Spear Phishing Email (Boss/ CEO): Phishing Emails with attachment or File Download



Sender: CEO <bill.jonson99@hotmail.com>

To: me

Subject: Urgent payment

Hi, Jane,

I am at the meeting now for a few hours and have limited access to my work email and to my mobile phone. I just got a message informing that we are late with payment to our exclusive partner.

In order to get goods on time, **please do urgent payment today**

to the partner's supplier directly.

Bank details indicated below:

AA 12 3000 9852 0001 0020.

Purpose of payment: for goods

Counting on you,

Bill Jonson

Sender: Managing Director <Eva.Stivens53@yahoo.com>

To: me

Subject: Current Month Salaries

Hi, Tom,

I'm working from home today, therefore I'm writing from my personal email.

I updated salaries of current month and made several changes. I am sorry for this misunderstanding, hope you will be able to make the changes and all staff will be paid on time.

Contact me, if you have any questions.

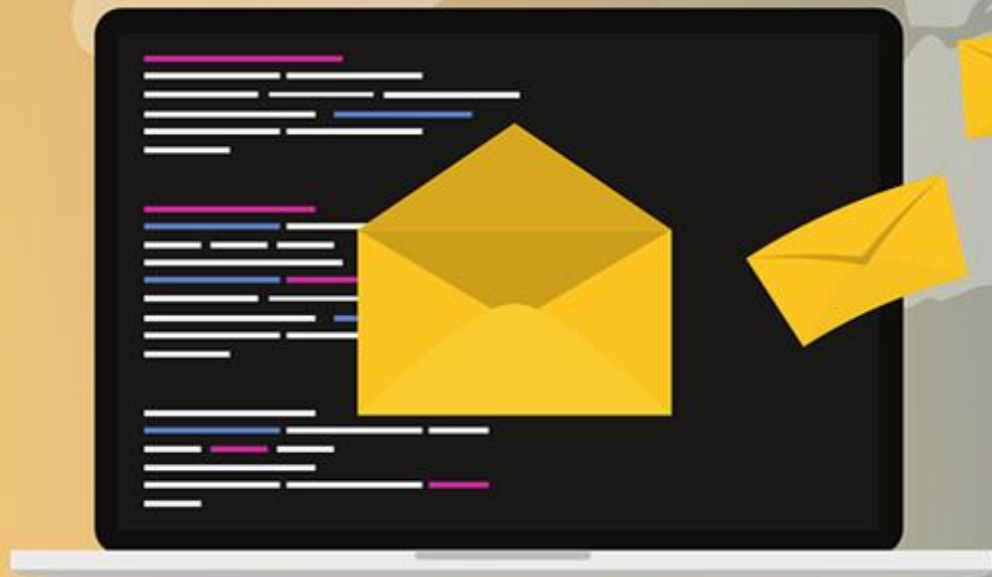
Regards

Eva Stivens, Managing Director

Updated-Salaries.xls



Tech Support Phishing Emails



Phishing: Tech support

- **Why this type of attachment is successful?**

By using digital devices users usually get various errors or warnings. Therefore, scammers could claim tech support and offer help to solve security breaches through remote access software or by clicking a link in the email

- **Target:** all citizens, especially people not having digital skills, elderly people

- **Threat:**

- phishing attacks copy our existing workflows
- attackers ask to click provided link in the email or call provided phone number

- **Phishing tactic:**

- Emails regarding compromised email addresses or passwords
- Emails regarding shared documents for collaboration
- Emails informing about technical problems

- **Phishing factor:**

- Inspiring sense of urgency
- Inspiring sense of scare
- Attackers prey on emotions and instincts of the victim

- **Vulnerabilities:**

- citizens with limited or any knowledge about phishing

- **Result:**

- Ransomware, infected digital device, got access to the digital device, by having access to device scammers could use it for later attacks, change device settings, could steal sensitive data, user could loss money etc.

Attackers also could use another type of techniques:

Pop-up messages

Fake websites (about fake websites see in [Website phishing section](#))

Unexpected calls (about vishing see in [Vishing section](#))

Example of Tech Support Phishing Email



Sender: Mail Settings <tech-support.954mail-delivery352477@cloud.website.com>

To: Lucy Bradson

Subject: Email Delivery Failure

Hello lucy.bradson

Email Server is having problem verifying your email.

You won't be able to receive new mails until you verify this mailbox.

Automatically Verify your mailbox now through below instruction.

[UTO-VERIFY MAILBOX NOW](#)

Your email account will be TERMINATED after 24hours if no valid action is taken.

Best Regards, Mailbox Administrator

Tech Support Phishing Calls



Example of Tech support phishing pop-up

Microsoft Security Alert



Your computer may have a Virus.

You have immediately to call
1 877 00 11 00 145 for assistance.

Your IP address:
147.254.114.741

Date:
11th February 2021

Phishing Emails: Romantic Relationship (Cat Phishing)

- **Why this type of attackment is successful?** There are people which are alone, divorced. They could get phishing emails or social media messages from scammers or they could be from dating websites.
- **Target:** alone, divorced people, people looking for new relationship, social media users
- **Threat:**
 - Scammers with fake identity, goes fast to relationship and get the trust of victim. After that scammers asks for money and vanishes after receives it.
- **Phishing tactic:**
 - Email from unknown person
 - Text message via social media, instant messaging programme
- **Phishing factor:**
 - **Go fast into relationship**
 - **Get trust of victim as soon as possible**
- **Vulnerabilities:**
 - emotionally vulnerable citizens
- **Result:**
 - financial loss.

Example: Romantic Relationship (Cat Phishing)

Sender: John John <john.19850215@gmail.com>

To: me

Subject: to my love

My Love,

I am very happy having the opportunity to find you, because only you in all the world could understand me. I feel that you are my second half. I believe that a thousand kilometers will not affect our close relationship.

I will make everything that I can to come to your country, change my workplace and spend the rest of my life in great happiness with you.

I look forward to your message.

Your Love, John

Sender: John John <john.19850215@gmail.com>

To: me

Subject: to my love

Hey, My Love,

You won't believe this, but I wanted to make you surprise and see you in your town. When I landed to Frankfurt, I had to wait for 18 hours for another plane. Therefore I went to the city hotel, and here my bag was stolen. Could you help me, please. I stayed in the hotel and tomorrow I need to cover Hotel invoice. Could you please cover my stay?

I look forward to see you asap, my Dear.

Your Love, John



Baiting



Baiting

- **Why this type of attack is successful?** People tend to trust and they believe that they could get something for free, buy something with discount, get money or prizes.
- **Target:** all citizens, including employees
- **Threat:**
 - scammers offer something very attractive, like to download music, movies, unexpected winning or awards, huge discounts and so on.
- **Phishing tactic:**
 - Email, pop-up, text message, social media posts with very attractive offer
 - USB drives lost near to office premises
- **Phishing factor:**
 - **False promise**
 - **Inspiring sense of greed**
 - **Inspiring sense of curiosity**
- **Vulnerabilities:**
 - Greedy or curiosity citizens, careless employees
- **Result:**
 - Get sensitive information, identity theft, intellectual property theft, sabotage, loss of money, installed malware.

Baiting Examples

Phishing Email: Discounts Scams

Sender: Black Friday Proposal<Black-Friday-Proposal@trust-fridays.com>

To: me

Subject: Congratulations! You've landed Secret Prices



BLACK FRIDAY!!!

**Access secret prices
up to 80 % OFF**

**Register to get
extra \$10 off**

www.trust-fridays.com/discounts/sdtuyx5D7rtkh6

Don't wait! The proposal expires after 5 days!

Unbelievably huge discounts or low prices of very well known brands and products

Baiting Examples

Phishing Email: Tax Refund and Covid-19

Sender: Government gateway <do-not-reply@online-gateway.com>

To: me

Subject: Government refund on COVID-19

To whom it may concern

The government has taken actions helping citizens and organizations suffering from Covid-19.

We inform you that you are eligible to get a one-time refund for \$2.500. In order to get this refund, you need to fill in this [online form](#).

This message was generated automatically by Government gateway

Scammers may follow real life events and use them for the attacks, they also could offer in-demand products or to recover taxes, like in this example.

Baiting Examples.

Phishing Email: Winning, Awards

Sender: Ade Goodchild <admin>

To: me

Subject: Dear Beloved

Dear Beloved,

Your E-mail was randomly picked by my foundation, you are to receive a donation 1,000.000.00 (One Million Pounds) which you must use at least 20% to touch the lives of the less privileged ones around you. I just kicked off foundation.

Read more details about how I became a millionaire.

<https://www.bbc.com/news/uk-england-hereford-worcester-47637306>

Kindly confirm the ownership of your email by sending your response to me immediately and I shall explain in detail you need to know.

Yours faithfully,
Ade Goodchild
Goodchild Foundation.



Baiting scammers could send emails informing victims about winning, awards and easy money.

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Text Messaging

- Short messages sent by phones, apps or social media platforms.
- Attackers could use such tactics:
 - Requests to send sensitive information in text message
 - Asks to click provided link in text message
 - Asks to open attachment
 - Call to provided phone number
- Usual topics of phishing text messaging:
 - Update personal or goods delivery information
 - Get huge discount or participate in the competition for prize
 - Account problems
 - Romantic relationship
 - Provide financial support

Text Messaging

- Text messages may be disguised as coming from reliable sources
- Phishing text messages could come via different platforms:
 - **Instant messages** (Hangouts, Skype etc.)
 - **Social Media platforms or apps** (Instagram, Facebook, LinkedIn, Snapchat, Twitter etc.)
 - **SMS phishing – smishing** (including WhatsApp, Telegram, Viber)
- Use shortening URL services

Text Messaging

Social Media and Instant Messaging (IM)

- **Why this type of attackment is successful?** It is difficult to distinguish from real messages (usually scammers use instant messaging worm, which infects devices after clicking link or opening attackment) etc.
- **Target:** all citizens
- **Threat:**
 - messages with attackments, with links, messages asking to perform financial support, messages from romantic scammers etc.
- **Attack method:** text messages from IM or social media contacts or unknown persons.
- **Phishing tactic:**
 - Short message (usually one or two sentences) with link. Messages asks to update account, change settings, open documents or pictures, suggest good discounts etc.
 - Short message (usually one or two sentences) with attackment.
 - Short messages asking for financial support
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **capitalising on naivety**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing and not expected to be phished via Instant Messaging
- **Result:**
 - Infected digital devices, identity theft, theft of credentials, loss of money

Text messaging

Instant Messaging (IM) Phishing Examples

John John

Did you see it???

Is it you in this photo?

<http://livegogle.com/images/family15.jpg>

Loren_18

Hi, watch my private video.
Don not share it to anyone.

<http://y2u-videos.info/Y7zNIEMDmI4>

Samantha

I am sharing online document with you:

<https://docs.google.com/document/d/ba?usp=sharing>

Sec-Admin

Your account is due to expire today. Please click link and activate your account

www.skype-admin.info/account-update?ID=7844156

Debbie Buorn

Would you like to know who viewed your Facebook profile?

Now it is possible. You need just to install app to your device.

Link to the app:
<http://bit.ly/38fCldxS>

Jim Lohan

You won 1.000 Eur gift card. Activate it

<https://bit.ly/3ALiAkE>

Text Messaging Social Media Phishing Examples



Hi, someone tried to login to your account several times unsuccessfully. Due security reasons, your account is locked. In order to unlock please sign in [here](#) and provide this code: **753147**

© Instagram, Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025




We found that you posted content which is encountered copyright. Your account was deactivated.

[Click here](#) to activate your account.

© Instagram, Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025



 <https://www.livegogle.com/images/family15.jpg>

© Instagram, Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

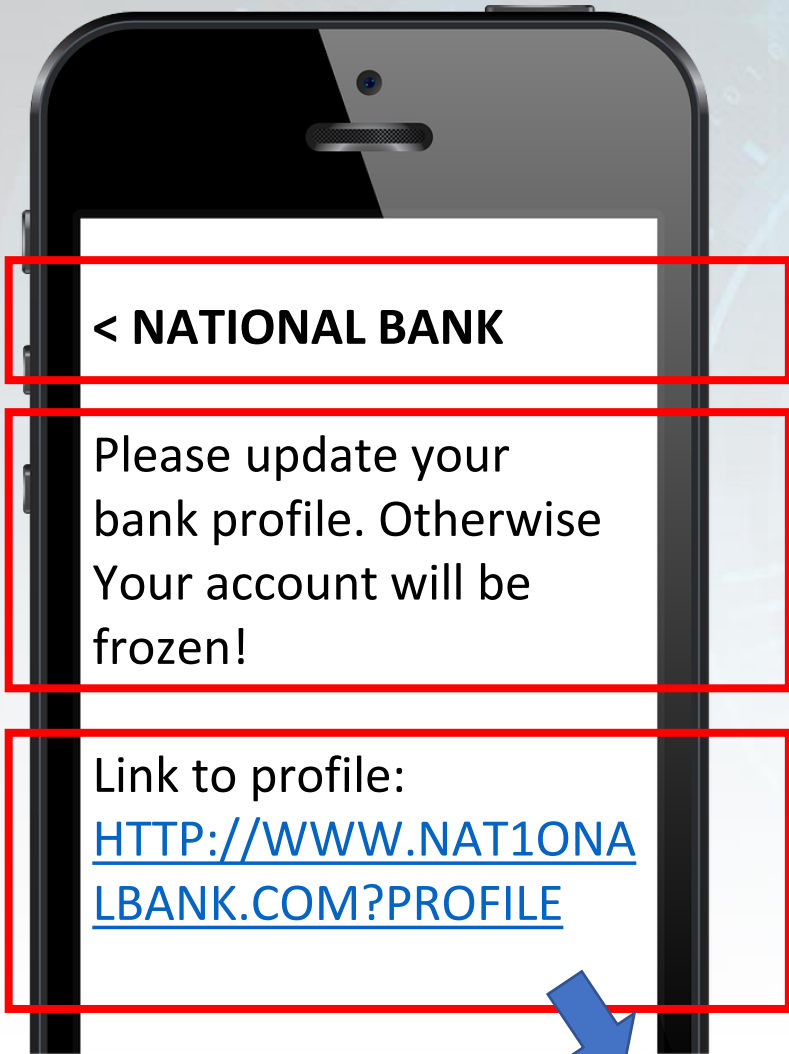
Smishing





Text Messaging: SMS (Smishing)

- **Why this type of attack is successful?** It is difficult to distinguish from real messages (usually scammers use real institution names).
- **Target:** all citizens
- **Threat:**
 - messages with links, messages asking to perform financial support, asking to reply or call
- **Attack method:** SMS text messages.
- **Phishing tactic:**
 - Short message (usually one or two sentences) with link. Messages asks to change settings, update account, change shipment data etc.
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **capitalising on naivety**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing and not expected to be phished via SMS
- **Result:**
 - Infected digital devices, identity theft, theft of credentials, loss of money

Text Messaging: Smishing Example



 <http://www.nat1onalbank.com?profile>

 **National Bank** **YOUR PROFILE NEEDS TO BE UPDATED!**

Name

Surname

Email Address

Email Address Password

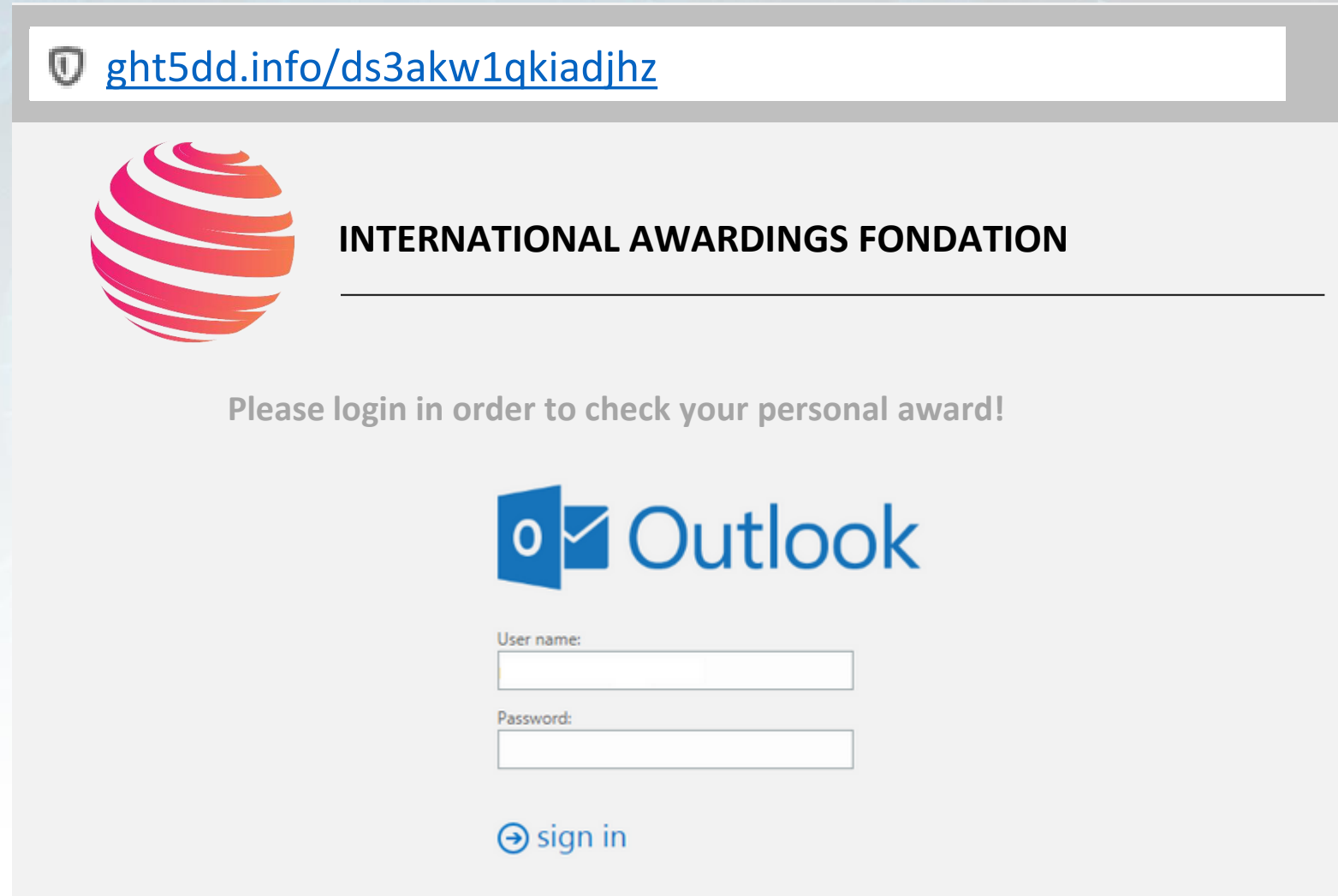
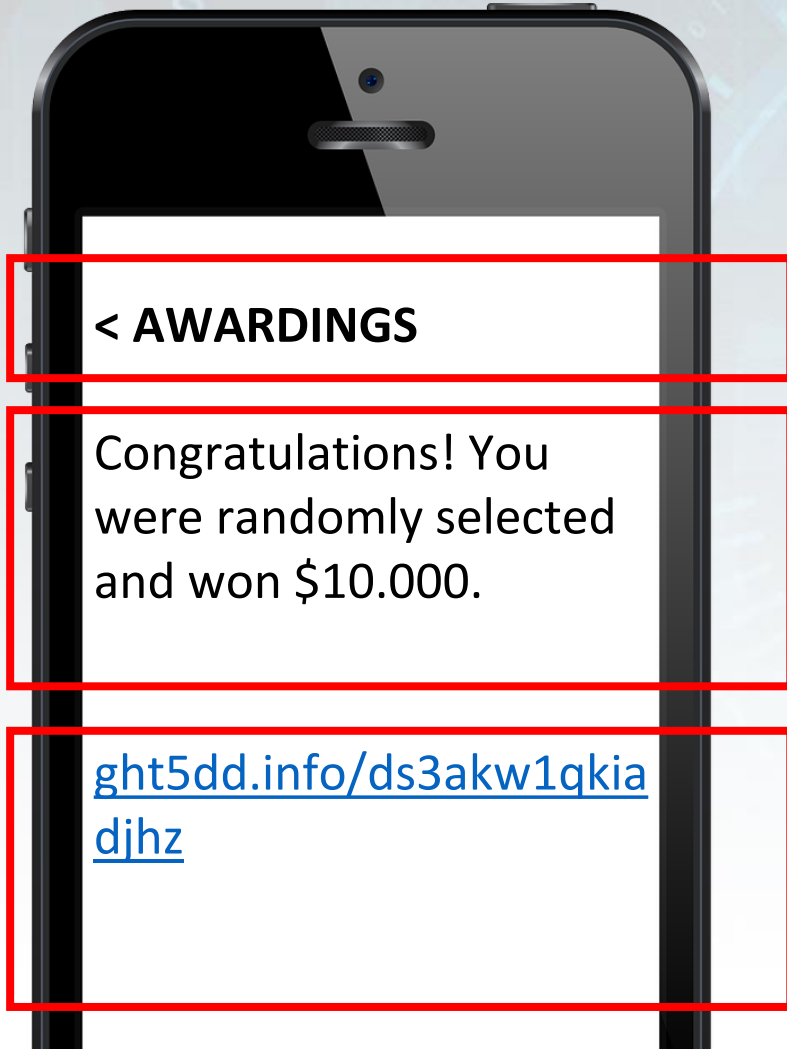
Credit Card Number

CSV Security Code

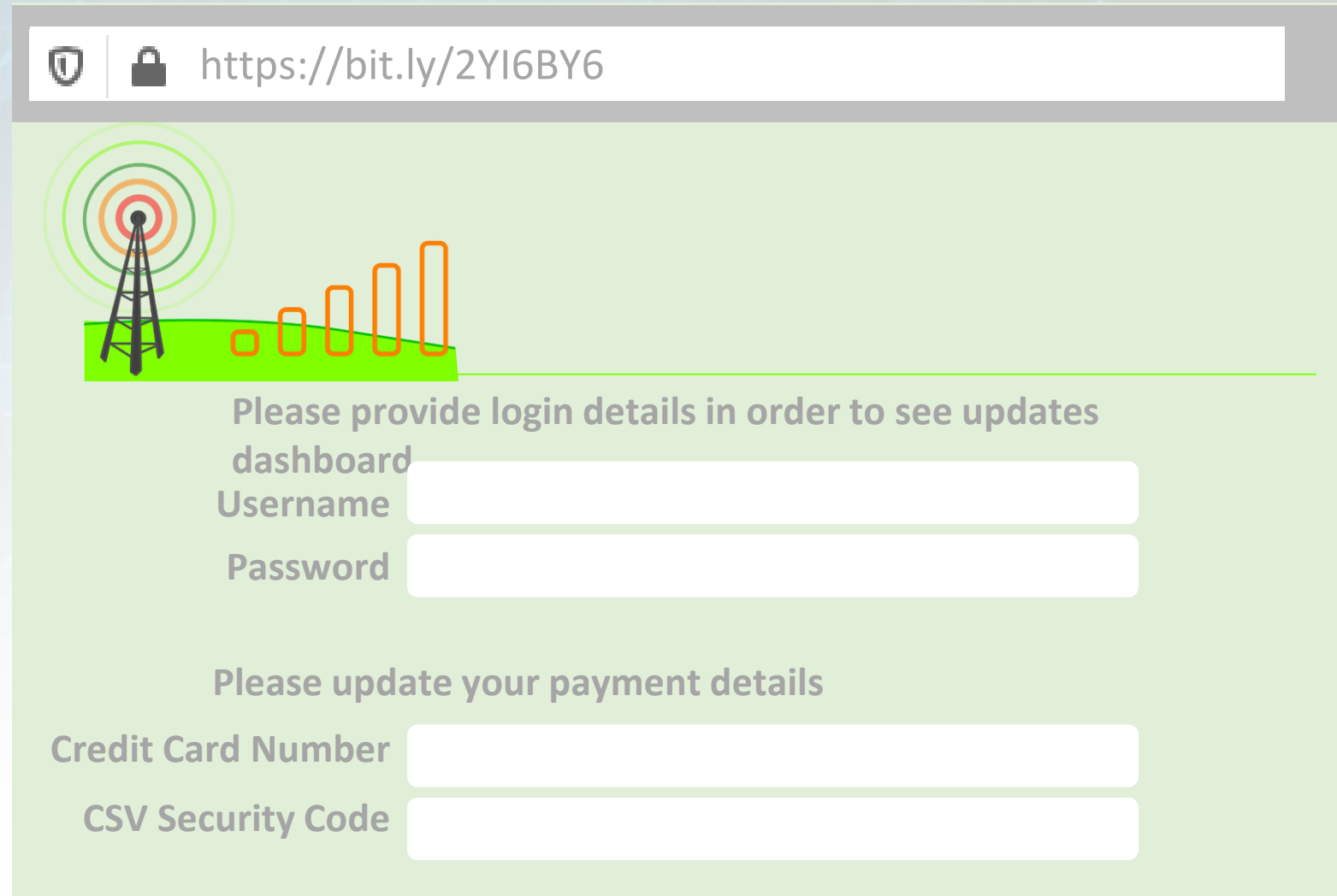
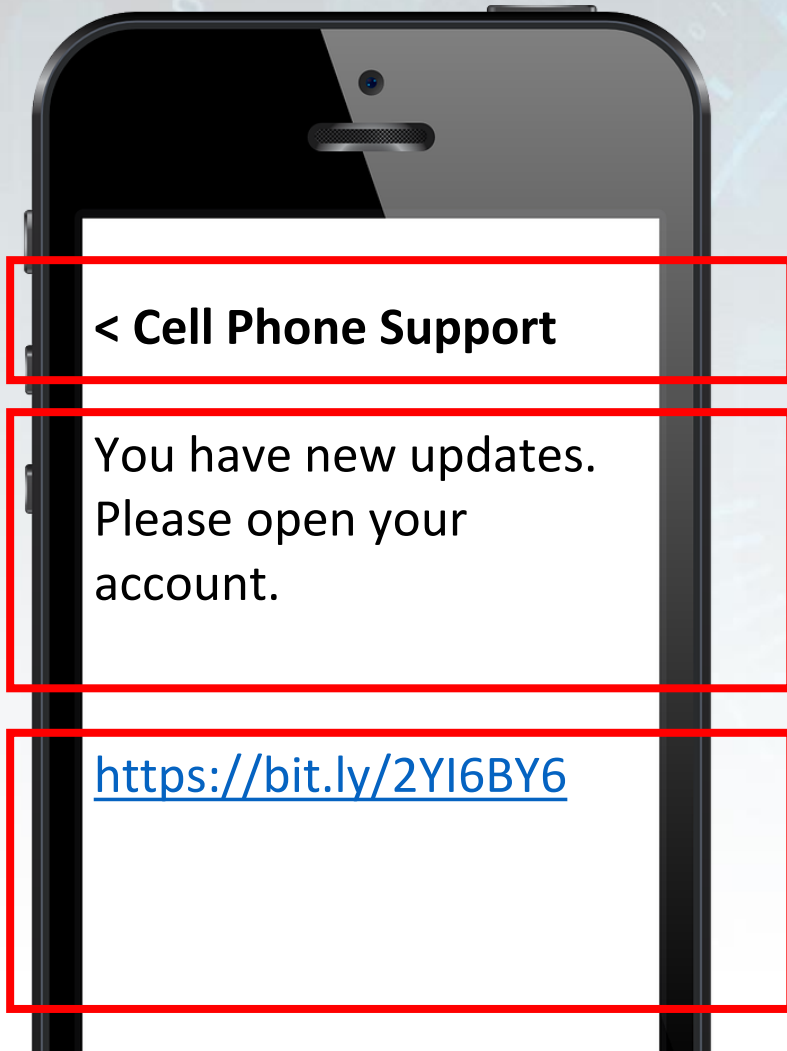
Update Your profile

<http://www.nat1onalbank.com?profile>

Text Messaging: Smishing Examples



Text Messaging. Smishing Examples



Text Messaging: Smishing Examples

< Post Services

Your shipment is ready for delivery. For instructions, please text to 9988 with code GET

Post Services

< Your Daily News

You are subscribed monthly news services successfully. In order to unsubscribe click:

<https://bit.ly/2YI6BY6>

< Municipality

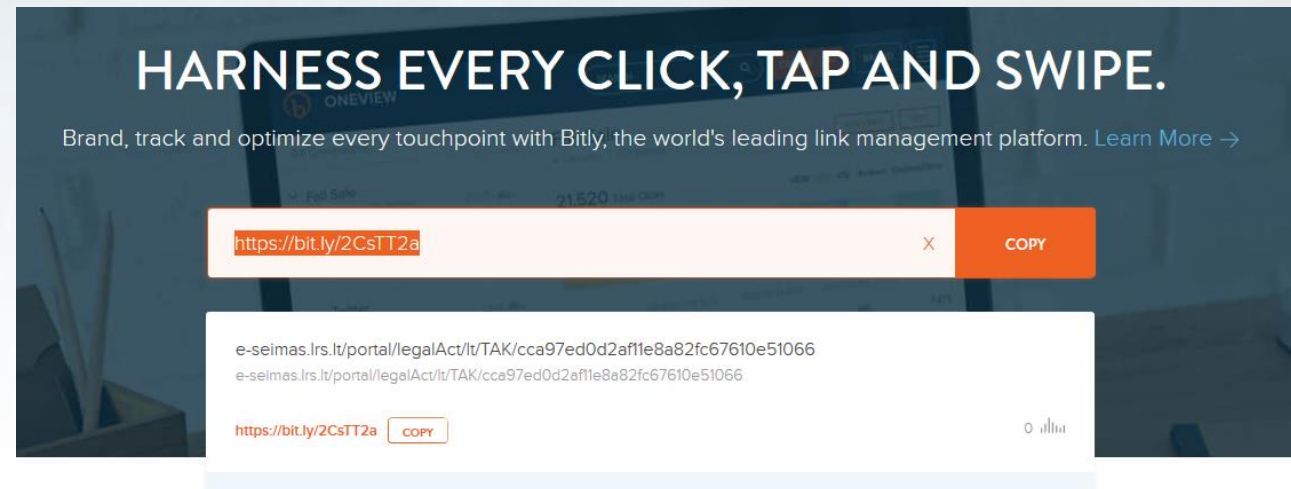
Your refund due overpayment is 1235 EUR

Please check for reimbursement

<http://www.International-bank.com>

URL Shortening Services

- URL shortening services are widely used. Examples of such services:
 - [Bitly](#)
 - [youtu.be](#)
 - [Rebrandly](#)
 - [TinyURL](#)
 - [BL.INK](#)
 - [URL Shortener by Zapier](#)
 - [Shorby](#)
 - [Short.io](#)



HARNESS EVERY CLICK, TAP AND SWIPE.

Brand, track and optimize every touchpoint with Bitly, the world's leading link management platform. [Learn More](#) →

`https://bit.ly/2CsTT2a` X COPY

e-seimas.lrs.lt/portal/legalAct/lt/TAK/cca97ed0d2af11e8a82fc67610e51066
e-seimas.lrs.lt/portal/legalAct/lt/TAK/cca97ed0d2af11e8a82fc67610e51066

`https://bit.ly/2CsTT2a` COPY

Purposes of Using URL Shortening Services

- Difficult to memorise long URL
- Convenient usage on websites, social media, printed publications
- Short URL convenient by sending SMS, instant messages
- There are shortening services providers, which can generate human readable URLs

Check bit.ly Link: at the end of link you can write +

← → ↻ 🏠 🔒 <https://bitly.com/3vfon0V+> ☆ 🛡️ ⬇️ 📄 📱 Ⓜ️ ☰

bitly ENTERPRISE RESOURCES ABOUT LOGIN SIGN UP

CREATED 10-15 18:35

Project Results – CyberPhish: Safeguarding against Phishing in the age of 4th Indu..

<https://cyberphish.eu/project-results/>

bitly.com/3vfon0V COPY

Check Information About Website



<http://checkshorturl.com>

Get long URL from hundreds of URL shortening services

Ensure your safety and prevent unsuitable content while surfing on the World Wide Web

<https://bitly.com/3vfon0V>

Expand

Long URL	https://cyberphish.eu/project-results/
Delay	0.96 second(s)
Short URL	https://bitly.com/3vfon0V
Redirection	301
Search long URL on	Yahoo Google Bing
Check if safe on	Web Of Trust SiteAdvisor Google Sucuri Norton
Title	Project Results - CyberPhish: Safeguarding against Phishing in the age of 4th Industrial Revolution
Description	N/A
Keywords	N/A
Author	N/A









Check Information About Website

- <http://www.getlinkinfo.com>: Determine if a website contains malicious software or is a phishing site



The screenshot shows the GetLinkInfo.com interface. At the top, the logo "GetLinkInfo.com" is displayed in blue. Below it is a search bar containing the URL "http://www.haitaoshou.com/data/system/lojin/" and a green "Get Link Info" button. A note below the search bar says "Enter any URL, for example: http://tinyurl.com/2unsh, http://bit.ly/1dNVPAAW".

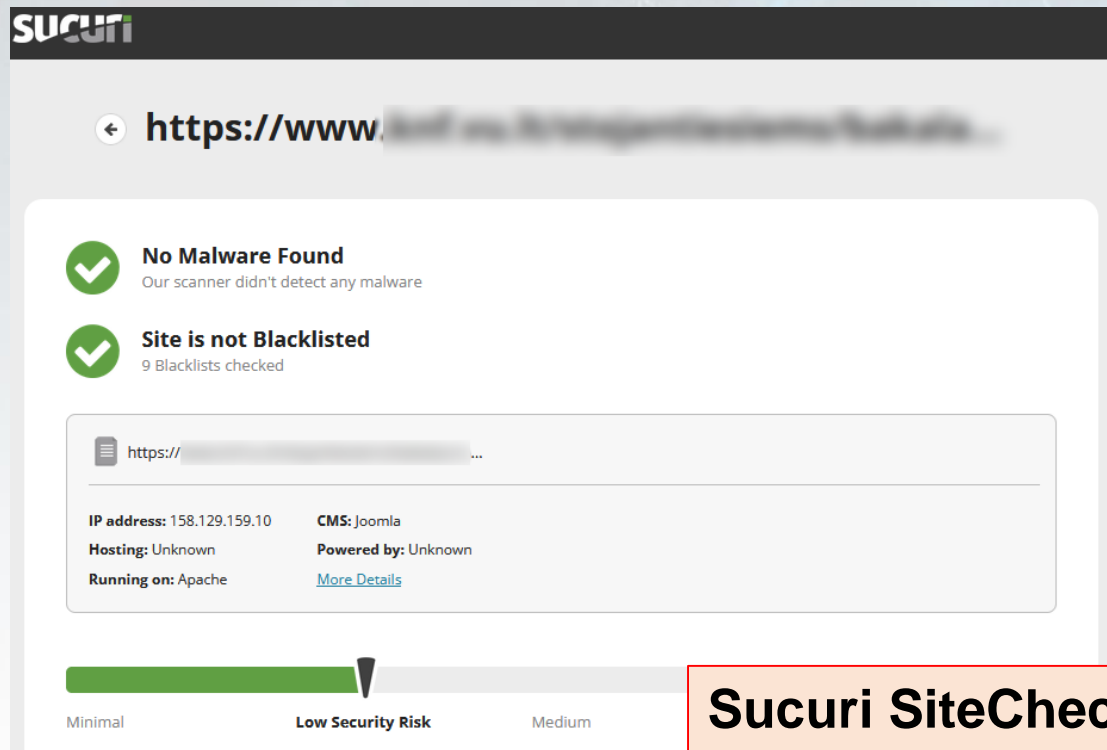
Link Information

 Title	(none)
 Description	(none)
 URL	http://www.haitaoshou.com/data/system/lojin/ <small>more info</small>  Unsafe
 Effective URL	http://www.haitaoshou.com/data/system/lojin/ <small>more info</small>  Unsafe
 Redirections	(none)
 Errors	404: Not Found. The page you requested was not found on the server.
 Safe Browsing	This site is malware-free and safe to visit. Advisory provided by Google

Check Information About Website

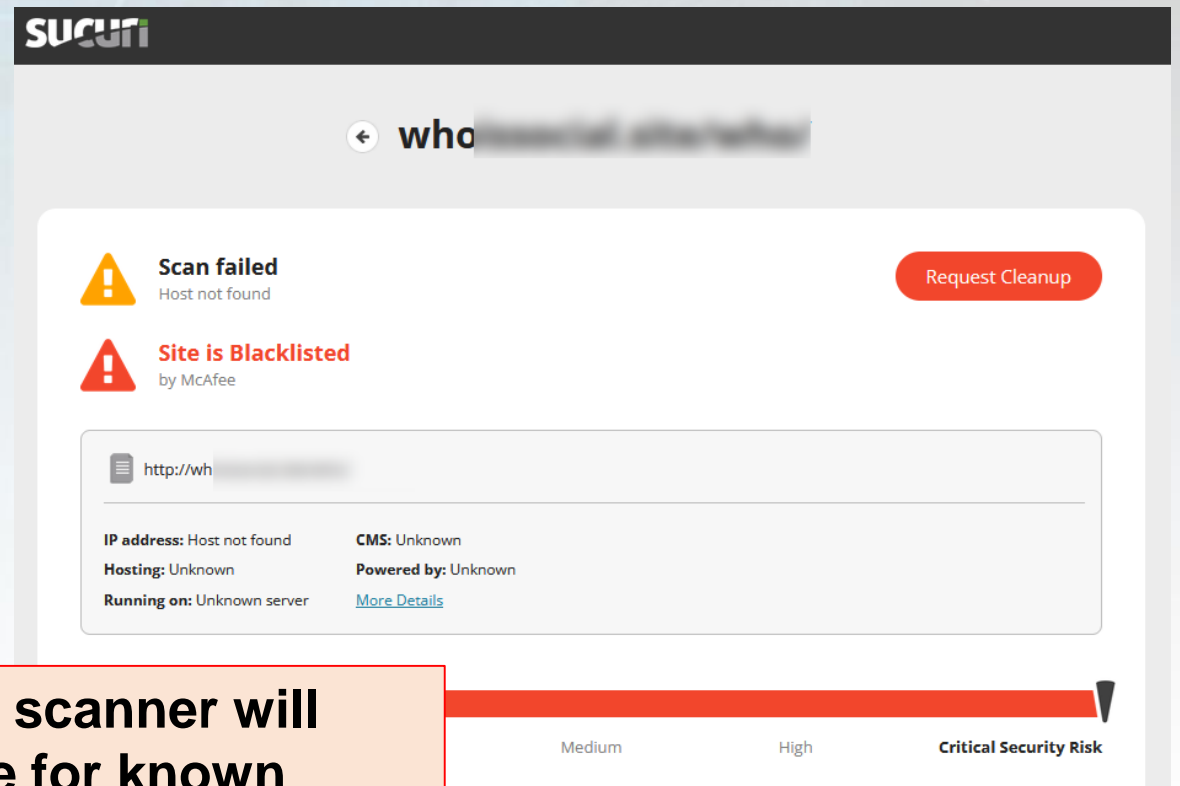
<https://sitecheck.sucuri.net>

Safe scanned website



The screenshot shows the Sucuri SiteCheck interface for a safe website. At the top, the URL is partially visible as "https://www.". Below the URL, there are two green checkmarks indicating a successful scan: "No Malware Found" (Our scanner didn't detect any malware) and "Site is not Blacklisted" (9 Blacklists checked). A technical details box shows the IP address as 158.129.159.10, CMS as Joomla, Hosting as Unknown, and Powered by as Unknown. A green progress bar at the bottom indicates a "Low Security Risk" level.

Unsafe scanned website



The screenshot shows the Sucuri SiteCheck interface for an unsafe website. At the top, the URL is partially visible as "who". Below the URL, there are two red warning icons indicating scan failures: "Scan failed" (Host not found) and "Site is Blacklisted" (by McAfee). A red "Request Cleanup" button is visible in the top right. A technical details box shows the IP address as "Host not found", CMS as Unknown, and Powered by as Unknown. A red progress bar at the bottom indicates a "Critical Security Risk" level.

Sucuri SiteCheck scanner will check the website for known malware, viruses, blacklisting status, website errors, out-of-date software, and malicious code.

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Website Phishing

- Website phishing is also called spoofing
- There are several types when phishing is used in websites
 - **Fake websites with fake URL** – fake copies of very well known institutions or organizations websites, which users trust*
 - **Self-operated websites** – scammers developed own websites, like fake web shop, investment portals*
 - Free hosting services
 - **Pop-ups** in the websites
 - **Advertisements' blocks** used in portals, even in trusted websites
- Links of fake websites are used in the phishing emails, SMS, instant messages, social media etc.
- Search engine also could provide links to dangerous websites*

* www.uni-mannheim.de/en/information-security/security-tips/spam-and-phishing/examples-and-current-warnings/#c230018

Website Phishing

- The main goal of such fake websites:
 - Get login credentials to information systems, emails
 - Get financial information, like bank card data and security codes
 - Infect users devices, because such websites may contain malicious code
- Scammers could use similar domain names to legitimate webpage, usually replace one or several letters in domain name, like using letter “l” instead of “i”; example:
 - Original website www.website.eu
 - Fake website www.webslte.eu

More about HTTPS:

<https://www.cloudflare.com/learning/ssl/what-is-https>

<https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/>

Website Phishing

- Fake websites use the same design, logos and colors like legitimate website, therefore it is difficult to recognize. Therefore other indicator should be checked, like:
 - URL address,
 - Contact details,
 - Be careful providing credentials or financial data when opening link from email.

Fake Website Address

- The URL of fake websites usually starts with HTTP
- Fake websites also could start with HTTPS
- HTTPS uses SSL certificate, verify ownership of website and keep user data secure: ensures secure data transmission between client and server, but not indicate that website is legitimate

More about HTTPS:

<https://www.cloudflare.com/learning/ssl/what-is-https>

<https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/>

Website Phishing

- **Why this type of attackment is successful?** It is difficult to distinguish fake websites from real websites, other phishing factors are used in order to inspire users to open websites, perform particular actions.
- **Target:** all citizens
- **Attack method:** emails, SMS, instant messages, social media posts, combined methods.
- **Phishing tactic:**
 - Email or message with link. Messages asks to update account, change settings, open documents or pictures, suggest good discounts etc.
 - Users can find fake websites by using search engine: it could be online store goods with good discounts
 - Scammers could call to victims inviting them to make successful investments
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **Instils greediness**
 - **Capitalising on naivety**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing and not expected to be phished
- **Result:**
 - Infected digital devices, identity theft, theft of credentials, loss of money

Website Phishing: Example of Phishing Website

 http://sale-branding.store



 Safe online shopping

BEST PRICES! ALL BRAND IN ONE PLACE WITH 90% DISCOUNT ONLY TODAY!



Funded by the
Erasmus+ Programme
of the European Union

Website Phishing: Example of Phishing Website



 http://mobile-company.online/prizes

CONGRATULATIONS!

Our company celebrates its anniversary this year, therefore we share the joy with our customers and invite you to collect your prize absolutely free.

Win one of the following prizes:

Samsung Galaxy S21, Apple iPhone 13 Pro or Samsung Watch 4 LTE.

153 participants are already enjoying their prizes. The number of prizes is limited!

Time reserved for you: **1 min. 29 seconds.**

I WANT TO RECEIVE MY PRIZE!

 http://mobile-company.online/iwantget

Samsung Galaxy S21

Price: 780 Eur

Out of stock

Not available

Apple iPhone 13 Pro

Price: 920 Eur

Only 2 items available

Get now!


Samsung Watch 4 LTE

Price: 320 Eur

Out of stock

Not available

Website Phishing: Example of Phishing Website

 www.face-account.book.online

Login in to Facebook

Email address or phone number

Password

Log in

[Forgot your password?](#)

Create new account



Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Lotteries Scams

- Lotteries scammers uses different tools to catch their victims:
 - Email
 - SMS or messages via instant messaging programs
 - Social media post from fake or hacked account
 - Call via phone
 - Web pages
- Victims are intended with huge amount of money, large prize, like cars, digital devices or other expensive goods
- They can introduce as legitimate lottery, agents or as a heir in need of assistance

Lotteries Scams

- Main signs indicating about lotteries scams*
 - You have to provide personal and financial information
 - If scammers ask to pay particular amount of money in order to increase chances of winning
 - You have to pay particular fees to get your prize
- Lotteries scammers expect to retrieve personal and financial information or trick to send them money like fees, taxes, shipping charger, inconsistencies between currencies or money for covering other expenses, pay with gift cards in order to get prize etc.
- They could ask to perform particular actions and do not disclose information about winning for a while i.e. keep it as a secret

* www.consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams

Lotteries Scamming

- **Why this type of attackment is successful?** It is difficult to distinguish fake websites from real websites, other phishing factors are used in order to inspire users to open websites, perform particular actions.
- **Target:** all citizens
- **Attack method:** emails, SMS, instant messages, social media posts, combined methods.
- **Phishing tactic:**
 - Email or message with link. Messages asks to update account, change settings, open documents or pictures, suggest good discounts etc.
 - Users can find fake websites by using search engine: it could be online store goods with good discounts
 - Scammers could call to victims inviting them to make successful investments
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **Instils greediness**
 - **Capitalising on naivety**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about phishing and not expected to be phished
- **Result:**
 - Infected digital devices, identity theft, theft of credentials, loss of money

Example: Lotteries Scamming

Sender: National lottery<jim-Stanley@info-winlottery.online>

To: me

Subject: Congratulations!

Dear user,

we would like inform that your email was selected to claim the sum of 150.000 EUR.

In order to get your money please follow attachment instructions.

*National lottery team
CEO Jim Stanley*



Instructions-for-winners.pdf

Other lotteries examples provided in the following slides:

- [Email section](#)
- [Instant messaging slide](#)
- [SMSishing slide](#)
- [Website phishing section](#)

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Phone Calls: Vishing

- Vishing could be explained as voice phishing
- Attackers use elaborated scenarios and scripts to gain victims confidence
- Vishing could be combined with other social engineering methods
- Sometimes attacker could make research before calling to a victim, in order to get more confidence



Phone Calls: Vishing

- **Why this type of attack is successful?** It is difficult to distinguish fake calls from real calls. Attacker represents himself as another person or representative of legal institution, like police or bank and without using any other technical tools except a phone, uses manipulations, exploits human fears, authority or desires in order to get sensitive information .
- **Target:** all citizens
- **Attack method:** calls via phone, calls via instant messaging programs, like Viber. Attackers could combine other techniques, like fake websites.
- **Vishing tactic:**
 - Scammer pretending as a legal organisation employee usually calls to victim and provide investment possibilities; scammers could pretend as a representative from police, scare victim with financial machinations on his account in order to gain access to the victim's bank account.
- **Phishing factor:**
 - **Inspiring sense of urgency**
 - **Inspiring sense of scare**
 - **Instils greediness**
 - **Capitalising on naivety**
- **Vulnerabilities:**
 - citizens with limited or any knowledge about vishing
- **Result:**
 - loss of money

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

Phone calls

Face to face

Shoulder surfing

Face to Face: Tailgating

- Tailgating attacks also referred to as “piggybacking”, is used when cybercriminal exploits company’s employees to get inside the organisation’s restricted premises
- The access to the restricted area is allowed only for authorised personnel



Face to Face: Tailgating

- **Why this type of attack is successful?** In huge organisations employees could do not know other colleagues, people tend to trust strangers.
- **Target:** employees in organisations
- **Attack method:** attacker could pretend as a new employee, as a service provider, as a goods delivery assistant etc.
- **Tailgating tactic:**
 - Cybercriminals simply trick and fool one of the authorized employee by following behind him/her for an entry.
 - The attacker could pretend being a delivery agent holding several boxes, meal delivery man and asking personnel to open the door.
 - Another example of this attack could be pretending to be companies' employee and start conversation in public company areas, like smoking areas. After the break pretender could go together with a chosen employee indulged in conversation while following him inside the restricted area.
- **Tailgating factor:**
 - **Inspiring sense of urgency**
 - **Inspiring confidence**
 - **Capitalising on naivety**
- **Vulnerabilities:**
 - employees with limited or any knowledge about tailgating
- **Result:**
 - Huge amount of damage could be caused when unauthorized person gets into the restricted area.
 - When outsider gets into the restricted area, he can perform an attack, like data theft, data breach, malware attacks and so on.

Contents

Event-based attacks

Emails

Text messaging

Websites

Lotteries scams

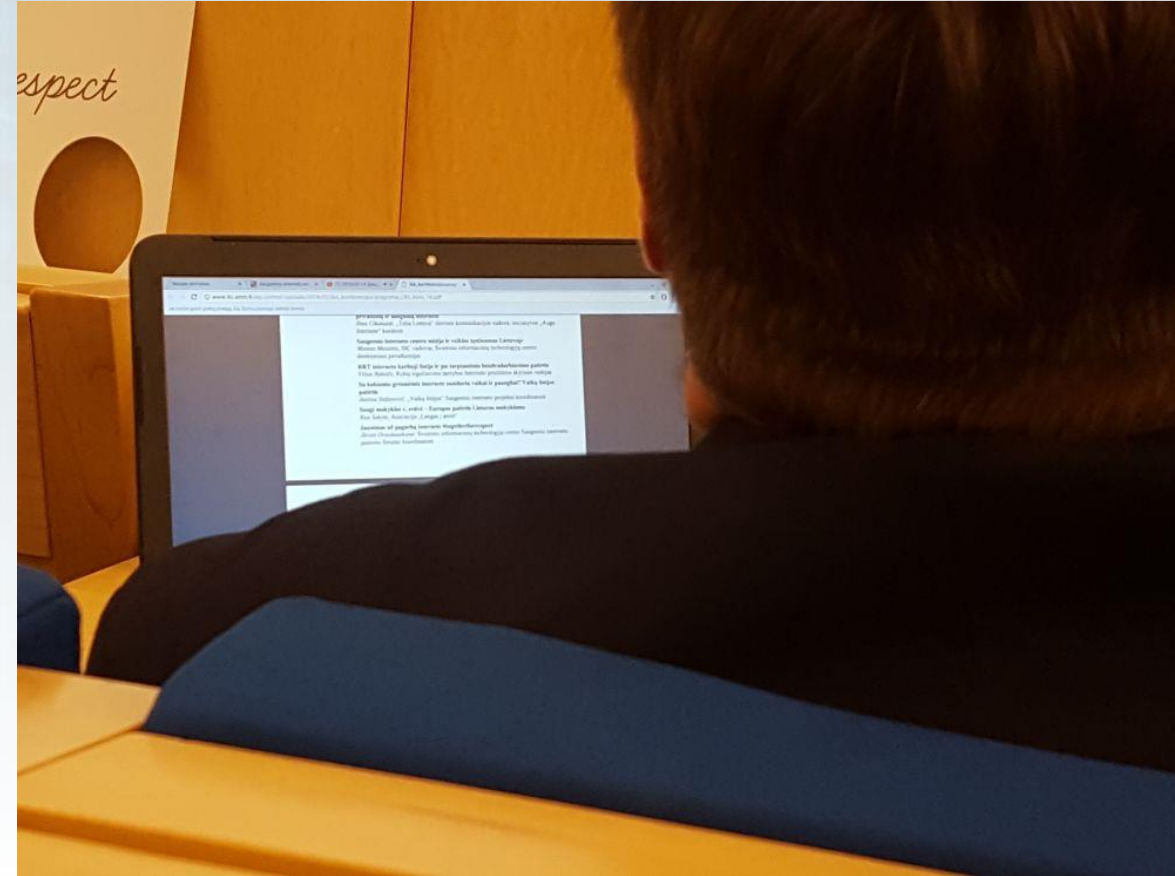
Phone calls

Face to face

Shoulder surfing

Shoulder Surfing

- Shoulder surfing is an effective way to monitor someone's computer, smartphone or ATM screen in order to get personal login to the systems data, like logins and passwords, PINs or other sensitive information
- The attacker can observe by standing near to the screen, listening verbally provided sensitive data or also the attacker can use web-cameras in order to collect necessary data

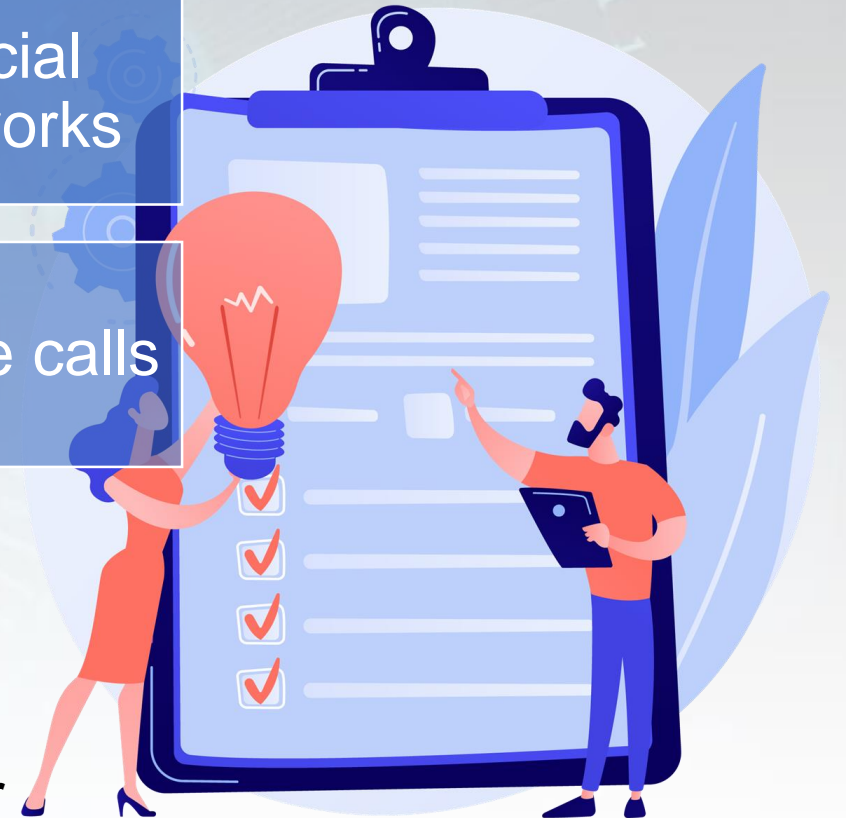


Face to Face: Shoulder Surfing

- **Why this type of attack is successful?** People who usually work with laptops and smart devices in public areas, at public events, on public transport do not think about the fact that someone might be watching his or her screen and don't think about the consequences.
- **Target:** all citizens
- **Attack method and tactic:** the attacker can pretend to be a normal person sitting or standing next to the victim, but is actually watching the victim's screen and collecting sensitive user data. To avoid arousing suspicion, scammers may use webcams.
- **Tailgating factor:**
 - aims to inspire confidence
- **Vulnerabilities:**
 - citizens with limited or any knowledge about shoulder surfing
- **Result:**
 - stolen personal login to the systems data, like logins and passwords, PINs or other sensitive information.

Summary: Phishing Attacks

Event-based attacks	Emails	Instant Messaging	Social networks
Websites	Lotteries scams	SMS	Phone calls
	Face to face	Shoulder surfing	



Scammers and attackers consciously improves their used techniques or use combination of techniques

Assignment



- Discuss what types of phishing attacks do you know
- Have you ever faced a phishing attack? What type was it?
- What do you think which type of phishing attack is most popular?
- What could be results of successful phishing attack?
- List at least four different phishing factors

Further Reading

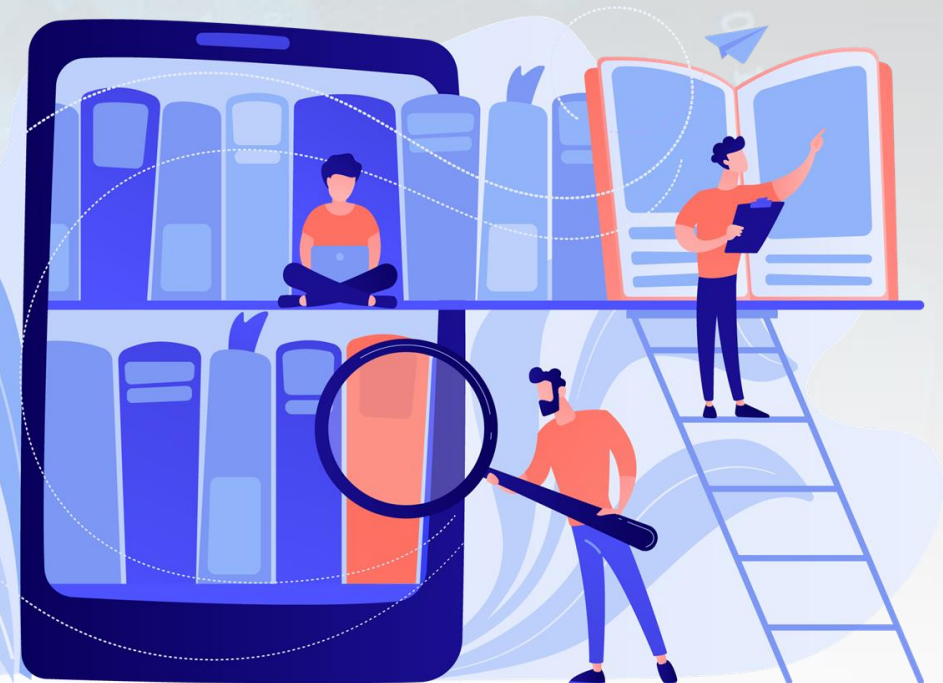
Christopher Hadnagy (2018). *Social Engineering: The Science of Human Hacking* 2nd Edition.

Erdal Ozkaya (2018). *Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert.*

Martinez, Claudia. *Defending Against the \$5B Cybersecurity Threat - Business Email Compromise.* Cisco Blogs available at <https://blogs.cisco.com/security/defending-against-the-5b-cybersecurity-threat-business-email-compromise>

Tusan, Christina. *Fake emails could cost you thousands.* US Federal Trade Commission available at <https://www.consumer.ftc.gov/blog/2017/05/fake-emails-could-cost-you-thousands>

US-CERT. *Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks.* US Department of Homeland Security available at <https://www.us-cert.gov/ncas/tips/ST04-014>



Short Videos

- What is phishing? Learn how this attack works
<https://youtu.be/Y7zNIEMDml4>
- What Is A Phishing Attack? And How To Avoid It
<https://youtu.be/j3nE8JQATXo>
- Learn how to spot phishing and spam email
<https://youtu.be/AmPX4DdBz-k>
- What is Spear Phishing | Difference from Phishing and Whaling
<https://youtu.be/JzoJeJBdhul>
- What is smishing? How phishing via text message works
<https://youtu.be/ZOZGQeG8avQ>
- What is vishing? Understanding this high-tech phone scam
<https://youtu.be/DysFLnOf4Nw>
- What Should I do if I Accidentally Click on a Phishing Link?
<https://youtu.be/d21-z8wsO7c>



Thank you!



Resources of pictures used in the presentation from:

- www.pixabay.com
- Personal archives

Screenshots made from websites