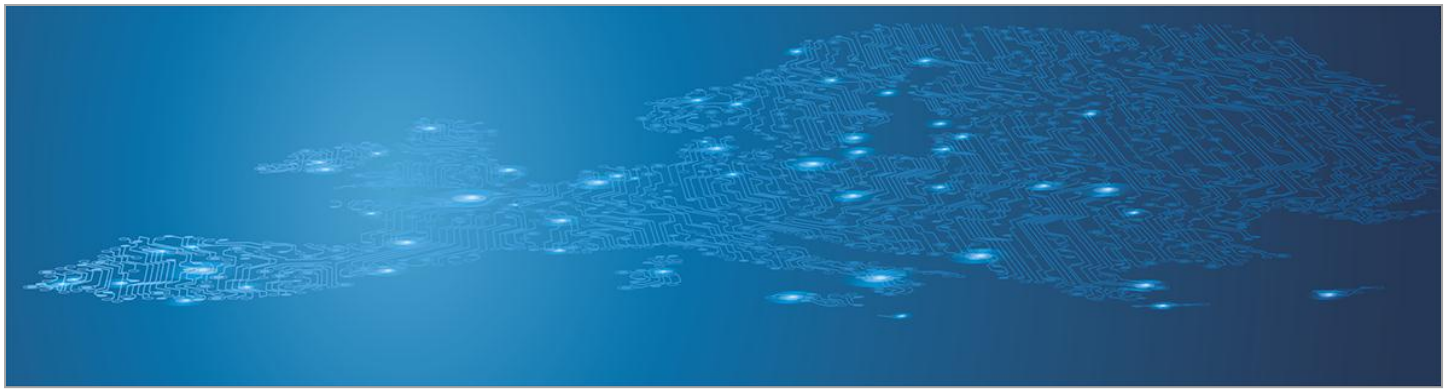


Incident handling and cooperation during phishing campaign

Handbook, Document for teachers

September 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This document was created by the CERT capability team at ENISA in consultation with:

Don Stikvoort, Michael Potter and Alan Thomas Robinson from S-CURE, The Netherlands, Mirosław Maj, Tomasz Chlebowski, Paweł Wężgowiec from ComCERT, Poland, Przemysław Skowron from Poland, Roeland Reijers from Rubicon Projects, The Netherlands and Mirko Wollenberg from DFN-CERT Services.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this document, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors:

- Toomas Lepik from CERT-EE, Estonia, Andrew Cormack from JANET, United Kingdom, Anna-Maria Talihärm from Estonia, Jim Buddin from TERENA, The Netherlands
- The countless people who reviewed this document.

Legal notice

Copyright Notice

ISBN 978-92-79-00077-5 doi:10.2788/14231

Table of Contents

Main Objective	This exercise treats phishing on three levels: technical, organisational and legal. The purpose is to understand phishing campaigns better and understand how to resolve them in complex international contexts.	
Targeted Audience	National CERTs, bank CERTs, CERTs for big companies or organisations: all CERT team members benefit from a better understanding of phishing and fighting phishing, but those in a 'front line'/operational role, and those who create policies would especially benefit from knowing how phishing works and how to cooperate to fight phishing.	
Total Duration	~ 4 hours plus 30 min breaks	
Time Schedule	**Introduction to the exercise**	15 minutes
	Task 1: Phishing Messages	65 minutes
	Break	15 minutes
	Task 2: Infection Mechanisms	80 minutes
	Break	15 minutes
	Task 3: Phishing Role-play	105 minutes
Frequency	Annual	

1 General Description

Mitigating and efficiently resolving a phishing campaign is a complex task; therefore it is extremely important to approach it in a coordinated manner. For this reason it is necessary to analyse a phishing campaign through all of its phases as shown in the figure below.

Figure 1: Main phases of phishing attacks

By the end of this exercise, trainees will have a greater understanding of:

- Phishing mechanics (infection vectors, infection mechanisms, fraud mechanisms).
- Organisational measures against phishing.
- Cooperation between CERTs on different levels, law enforcement and security providers in different countries to resolve phishing cases.

2 Exercise Course

This exercise is best conducted by a trainer plus a co-trainer.

The exercise allows the trainees to first investigate some of the mechanisms involved in phishing, as an introduction to a role-play in which they explore an international phishing case, involving various CERTs and law enforcement agencies. This is to discover how a phishing case could be coordinated and resolved, including the aspect of cooperation with law enforcement.

Both the trainer and co-trainer need to prepare for the exercise well. This is best done by reading this handbook text thoroughly and thinking through the requirements for the room layout, the accompanying materials, hand-outs and projected slides. When you do this for the first time, we advise the trainer and co-trainer to conduct a (shortened!) dry-run with the trainer in the trainer role, and the co-trainer in the trainees' role(s), thus seeing together how the exercise works in practice. Also, it is advisable that the co-trainer takes care of exercise timing and the hand-outs, so the trainer can focus on the trainees and the few slides he or she needs to present. Once the trainer and co-trainer have done this exercise once or twice, it will flow naturally. This is the authors' experience from giving similar role-play or discussion exercises.

Trainees are allowed to use laptops or handhelds to connect with the Internet to do fact finding during the exercise, whenever this supports the exercise. This will be indicated below by the text 'Internet use allowed'.

The trainees will be divided into 7 groups, preferably with a total of 14–21 participants, but no more than 28. The groups will stay together for the duration of the exercise. The groups will function in 3 ways – research/discuss within the group, take part in a role-play, and also participate in plenary discussion. The co-trainer makes sure that the groups are positioned so they can stay in place for all 3 functions. For the role-play to work well, the groups should preferably be located at equal distances spread over an imaginary circle. Each group should have a small table.

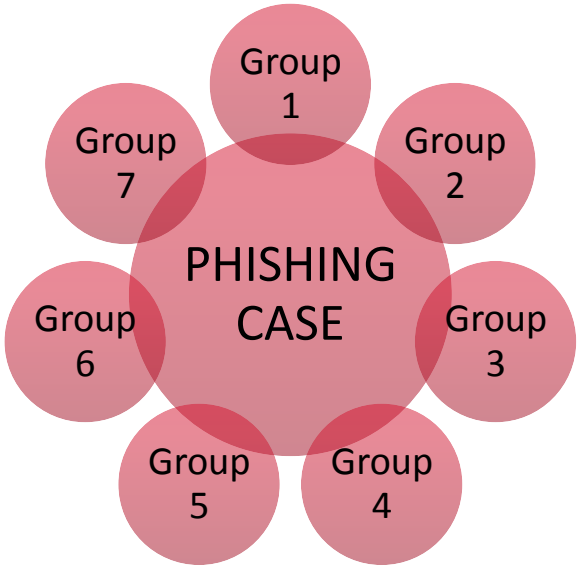


Figure 2: Group positions during the exercise

Note that included in this exercise is a rating for the groups, and the group that wins gets a special prize (to be prepared and decided by the trainers) – this is **optional** and intended to spice up the exercise. Some fun competition usually makes groups more active and fired up. Make sure it is **fun** competition though, and is not experienced as stress. The trainers need to set the right positive frame for such competition.

3 Introduction: 15 minutes plenary

The co-trainer makes sure that the trainees are divided into 7 groups and are positioned to enable group work, role-play and plenary discussion.
The trainer explains the goals of the exercise to the trainees:

- to explore the phenomenon of phishing
- to survey some of the mechanisms involved in phishing
- to perform a role-play in which the trainees explore an international phishing case, involving various CERTs and law enforcement
- to discover how a phishing case could be coordinated and resolved, including the aspect of cooperation with law enforcement.

The trainer then gives his or her own introduction into 'phishing' and dealing with phishing from the CERT perspective. If the trainer has personal experience with phishing and fighting it, bring that experience forward. The trainer can use some of the following information for his or her introduction – however bear in mind that the trainees need to discover some of the technical aspects below, so don't give them a tutorial, just make them curious:

- *Profitability of credit card and bank account fraud* (based on data from McAfee[1])
    - At the time of writing, a stolen credit card number is worth about €16 on the black market.
    - If the criminal also has the PIN and guarantees the account balance, then it's worth €130.
    - Banking account credentials are worth much more: a percentage of the account balance stolen. Example: the authors behind malware that steals bank account credentials can charge 2% of the account balance for US accounts to as much as 6% for EU accounts.
    - PayPal login credentials can net criminals 20% of the account balance.
- *Who does phishing?*
  Moderately clever criminals can create a fake ecommerce site to collect credit card information, or direct bank clients to a fake bank website, send any illicit proceeds through a series of banks worldwide until it reaches them, and then disappear.

[1] http://www.mcafee.com/de/resources/white-papers/wp-cybercrime-exposed.pdf *(2013)*

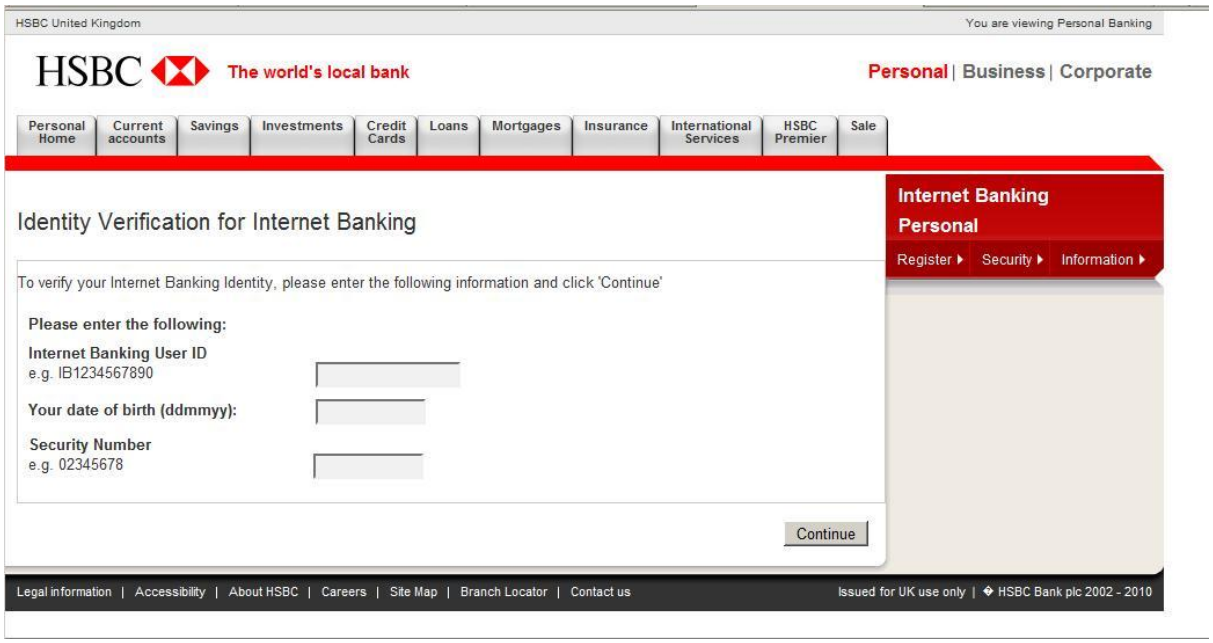


Figure 3: An example of a phishing site

- With profits as high as 6% of people's account balance, it is not surprising that capturing financial account credentials is the focus of sophisticated malware attacks by organised crime. Phishing and computer crime is out of the traditional 'hackers' hands – young, clever hackers are among the employees of organised crime. They are usually not the ones making the big money.
- *How hard is phishing?*
  The sensitive information stream from client to server is protected by mechanisms like SSL encryption. Let's look at the example of bank customers connecting with their bank. The bank servers themselves are protected and monitored quite well, on average – breaking in there is not impossible, but requires a relatively high investment in expertise and time. The weak spots are the client's computers, and the client's awareness. In general, phishing starts with an email[2] (or other infection vector like a USB stick, or downloading 'innocent' software). Clients are either seduced to visit a website that might take their credit card info, or are infected directly or via a website with malware. In the latter case, the malware (e.g. Blackhole kit[3]) may do just about anything – including rewiring DNS to direct the client to a fake bank site when they think they are going to their bank's site (DNS spoofing – see the graphical explanation below), or doing logging of anything they type in (like usernames and passwords), and/or making their computer a botnet zombie.

[2] *See e.g. http://www.phishtank.com/images/example_phish.gif or http://file.gov.com/graphics/phish_irs_spoof.gif*
[3] *http://sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf*

From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

Figure 4: An example of a phishing email

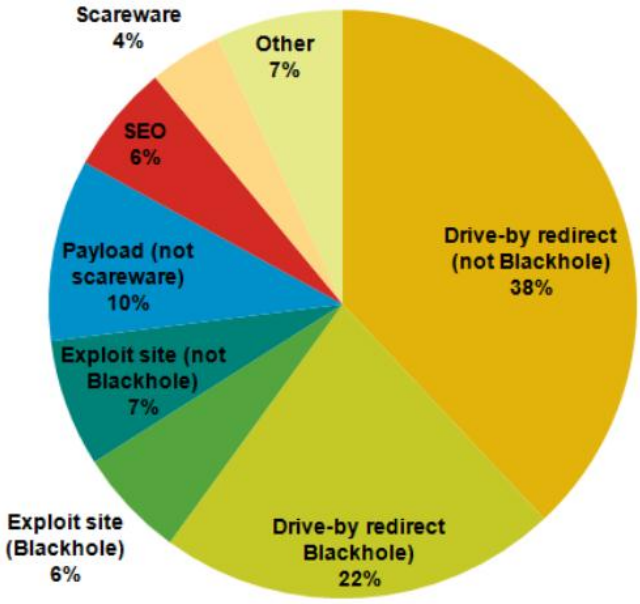


Figure 5: Breakdown of detected web threats by type with the relation to the Blackhole threat. (Source: Sophos Technical Paper: Exploring the Blackhole Exploit Kit[4])

[4] *http://sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf*

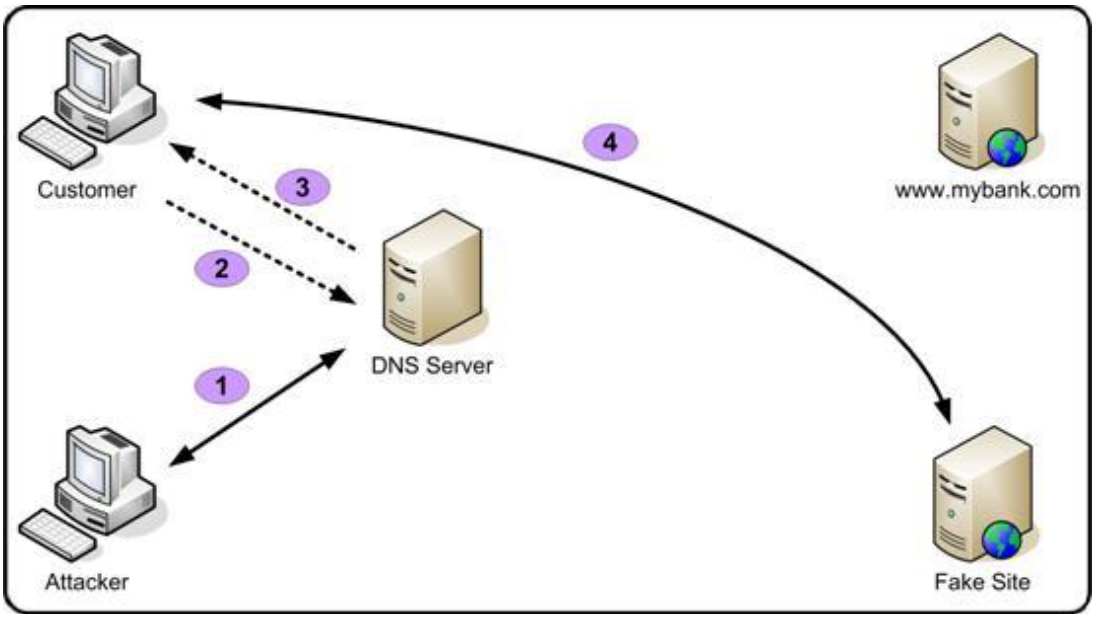


Figure 6: The DNS resolution process having fallen victim to a DNS spoofing attack (source: The Pharming Guide[5])

In the case of a fake bank site, the criminal has several options, for example:

- Some banks allow users to log in with username/password – and then perform financial transactions. In those cases, it is enough to simply let the client log in to what they think is their bank account, but is really a fake server run by criminals, collect the credentials and empty the bank account. Banks do have detection mechanisms for online banking activities or credit card processing which seem 'out of the ordinary'.
- For banks that use one-time passwords or token devices for every transaction, the criminals could use a man-in-the-middle attack. Their rogue server emulates the bank server towards the client and acts as client towards the bank server. If the bank asks for a code or password, the rogue server asks the client for the same. The client replies and the rogue server forwards it to the bank server. There is no way to detect this if the rogue server closely resembles the bank server except to examine the SSL server certificate.
- Other cases are those related to mobile threats, especially based on smartphone usage. To learn more about them see the ENISA exercise for CERTs number 16 – 'Mobile Incident Handling'.[6]

[5] http://www.technicalinfo.net/papers/Pharming2.html
[6] http://www.enisa.europa.eu/activities/cert/support/exercise/files/Mobileincidenthandlinghandbook.pdf

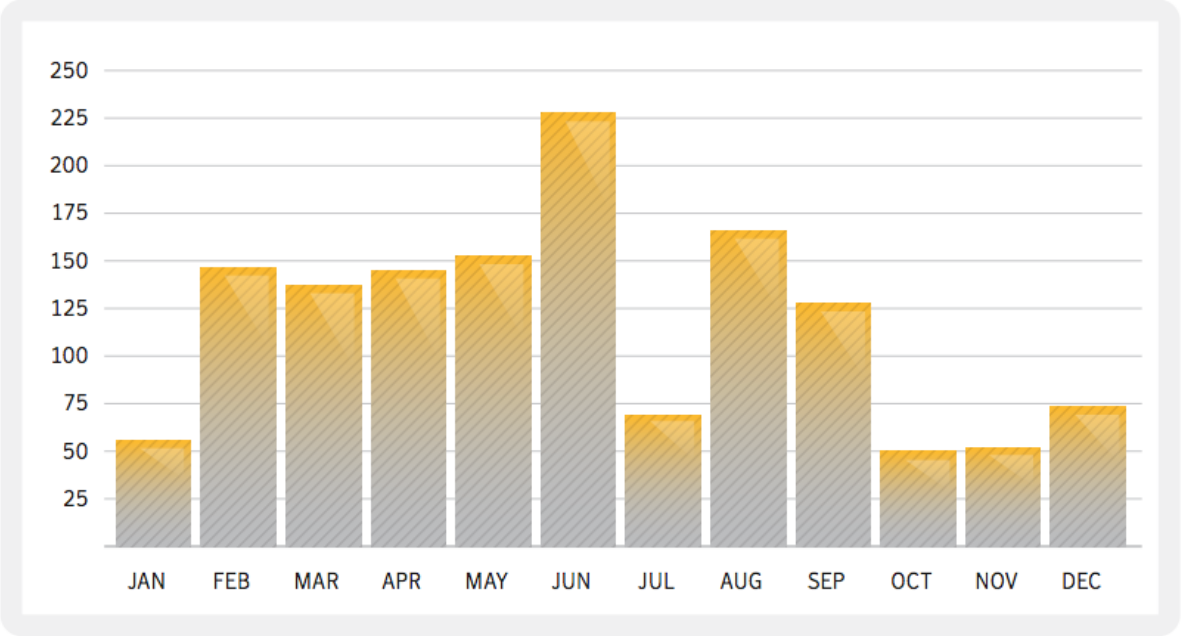


Figure 7: Mobile targeted attacks on clients of bank organisations per day in 2012[7]

- *Phishing vectors*
  Most popular vectors of infecting user device[8]:
  - Email with attached malware (masquerading as zip or picture or movie)
  - Email with links to web servers designed/adapted to infect client computers
  - USB sticks infected with malware
  - Downloads of popular software, offered in an infected version
  - Visiting popular websites which have been infected with malware. This has recently e.g. happened with one of the most popular web servers, Apache, by means of Darkleech.[9]
  - Mass infection of host service providers became popular in 2012[10] – this way many websites based on WordPress or Joomla, serving many domains, can be easily infected with phishing content/malware.

  Web servers as the source of malware look to be growing alongside more common vectors such as emails and infected files.[11] Web server infections are hard to detect. As such infections occur on legitimate websites, the usual IT advice of 'don't go to "bad" sites' to avoid malware does not help.

[7] *Symantec Internet Security Threat Report 2013 –* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf
[8] *According to authors and contributors recommendations and observations*
[9] http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/
[10] http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf
[11] http://arstechnica.com/security/2013/05/attack-hitting-apache-sites-goes-mainstream-hacks-nginx-lighttpd-too/

- *Other types of phishing.*
  We have discussed the obvious example of phishing attacks against credit card or bank account data. Of course online financial systems like PayPal are also subject to phishing. But the threat doesn't stop there. Targets are also customers of Gmail, Yahoo, Facebook, etc. This kind of phishing does not usually enable direct financial gain, but it can give access to resetting other accounts/passwords, like PayPal.
  According to Kaspersky 37 million users experienced phishing attacks in 2012[12] – the trainer is advised to read the short article referenced.

The trainer continues to explain the set-up used to reach these goals:

- Depending on the case and task at hand, hold general discussions with all trainees, or work in the small groups.
- The trainer, assisted by the co-trainer, will guide the various tasks and can at any time steer discussions or events (e.g. in a role-play) in any direction – the trainees can regard the trainer and co-trainer as the directors of the play they are all in.
- When working in groups, one trainee is assigned to take notes in each group – and another[13] group member may (or may not – depending on the exercise) be asked to present the findings and/or participate in a guided plenary discussion following the group work.

[12] http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year

[13] *If possible the one taking notes should not be the one presenting them – this is to maximise the participation of the trainees.*

4 Task 1 – Phishing Messages

The trainer gives a 5-minute introduction to the scenario that is used throughout this exercise (NOTE: this scenario will develop bit by bit during the exercise):

> *SUGARLOAF TRADING is a shipping company based in Cardiff in the United Kingdom. They ship goods worldwide, mostly using container traffic, via ships and trucks. Shipping involves financial transactions in many countries worldwide, as local agents do work for SUGARLOAF there, transport has to be paid for, customers billed etcetera. SUGARLOAF channels most of their financial transactions through their bank, CRIBGOCH BANK which is a UK bank.*

Figure 8: The Sugarloaf Company leaflet[14]

> *A spear phishing attack is targeted at several branch offices of the shipping company SUGARLOAF TRADING in the UK. The phishing attack uses emails, and aims at infecting SUGARLOAF TRADING employees' systems with malware. Now what do you think the spear phishers are after? (Open question to class – the answer is 'rob the bank accounts of SUGARLOAF, most likely', but other answers given can be discussed in brief)*

The trainer guides the groups to do the following 3 things:

(1) Devise, in their group, the most clever phishing email they can think of in the context described. The message really needs to convince employees of SUGARLOAF to do whatever the phishers

[14] *Appendix 3 has a copy of the leaflet if you want to print and hand it out to trainees.*

want them to do in order to get infected. This message needs to be written down. For this purpose mention some psychological methodologies as examples:

- Nigerian Scam – financial gain aspect;
- Letter from boss – management hierarchy aspect;
- Lottery winning – financial aspect;
- Hot news – curiosity aspect.

(2) Also, the group needs to describe briefly what infection mechanism is inherent or invoked in their phishing email, i.e. how the infection would take place and what malware might be involved.

(3) Finally, the group needs to describe in brief:

- the action that SUGARLOAF could take **inside** the company but also **outside** (coordinating with who?) when their IT/security people discover the attack behind the phishing email
- measures inside SUGARLOAF (and any company hit by a similar attack!) which might have prevented this specific attack – and similar attacks – from being successful

The trainers will rate each group by giving points out of 10 to the most convincing **phishing emails** – these points will add up during the whole exercise and the group that wins the most points gets a special treat (the trainers need to think of a special treat ahead of time!).

Detecting the phishing message can be based on the rules below. Use them for rating purposes.

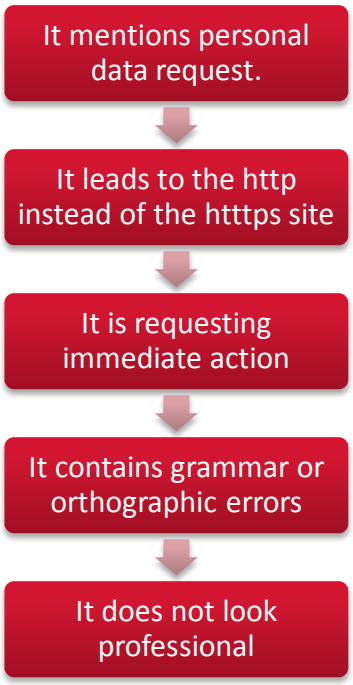


Figure 9: Simple criteria for rating phishing messages

The trainer says: **30 minutes in groups, ready, go.** Internet use **not** allowed

During the group work, the trainers go around and assess and rate the phishing mails as they are being completed. They select the top 3 for presentation.

When the group work is done, the top 3 read out their messages and explain the results of tasks (2) and (3) in brief. This will take up to 20 minutes.

The trainer finally uses 10 minutes to wrap up and if needed can use one or more of the phishing examples provided in Appendix 1 – Phishing mail examples. There is no need to discuss infection

mechanisms in greater detail as that is the next task. Measures to counter this kind of phishing in organisations could include: awareness raising campaigns, annual security training for select users, a policy to use email addresses only for business purposes and not for private mail, internal CERT and/or CISO as guardians.

While the trainer wraps up, the co-trainer finalises the group ratings and writes them on a chart or whiteboard – leaving room for the ratings yet to come.

15 minutes break.

5 Task 2 – Infection Mechanisms

The trainer gives a 5-minute introduction. The scenario is further developed:

> *As you know, several of SUGARLOAF's systems were infected as a result of the phishing emails. The infection mechanism used, for instance obfuscated scripts, enables malware designed for fraudulent aims. The malware here is aimed at gaining money from SUGARLOAF's bank accounts, via fraudulent online transactions involving CRIBGOCH BANK, the bank of SUGARLOAF. Remember, SUGARLOAF does many financial transactions worldwide, and channels these through their bank in the UK.*

The trainer guides the groups to:

(1) Research, in each group, one *infection mechanism* of the kind often used in phishing attacks: by *infection mechanism,* we mean the way that the infection actually takes place.

(2) Also, the group needs to write down:

- measures inside SUGARLOAF (and any company hit by a similar attack) which might have prevented this specific – and similar – infection mechanism from being successful
- ways in which CERT teams and Law Enforcement could assist in that,[15] e.g.:
    - Social response based on good awareness training for staff.
    - Technical responses based on measures implemented by local administrators as well as those implemented from outside solutions (e.g. browser alerting to fraudulent websites).

Each group is assigned one mechanism from the following list:

1. Blackhole kit[16]
2. Obfuscated script(s) on public web servers[17]
3. Zeus – Trojan horse that steals banking information[18]
4. Citadel – a variant of the Zeus mechanism
5. Hasperbot – Trojan horse that steals banking information[19]
6. Darkleech – the Apache module which installs malicious software on clients' machines[20]
7. Zeus via Facebook – the Zeus Trojan horse spread via Facebook service[21]

Note for trainers: feel free to adapt this list to your own needs and to new developments – just make sure to research them thoroughly.

The trainers will rate each group by giving points out of 10 for the most accurate analysis – these will be added to the points given before.

The trainer says: **30 minutes in groups, ready, go**. Internet use necessary.

During the group work, the trainers go around and make suggestions if needed.

---

[15] *A good listing of potential social, technical and legal measures can be found at Wikipedia's description of the phishing phenomena: http://en.wikipedia.org/wiki/Phishing*

[16] *Explanation presented by AVG Threat Labs. More information about the kit can be found at: http://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/*

[17] *The phishing scripts can be added to the WordPress sites. Example: -cgi-bin-wets-myapleid.woa-wa-direct.khanghorizons.com/MyAppleId.woz/9LImgDPxP0hAmTatec9Uaw/Verify-localang%3Den_US/ff2a09011035698ae7a4173c97d6536c/Login.php?login*

[18] *More: http://en.wikipedia.org/wiki/Zeus_(Trojan_horse)*

[19] *The virus technical explanation: http://www.welivesecurity.com/2013/09/06/hesperbot-technical-analysis-part-12/*

[20] *Darkleech: http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/*

[21] *http://www.techspot.com/news/52795-zeus-trojan-returns-facebook-being-used-to-spread-the-infection.html*

When the group work is done, all 7 groups explain, 4 minutes each, the infection mechanisms assigned to each of them. They can use a whiteboard or flip chart to support this. The trainers assess the ratings silently.

This will take up to 30 minutes including some interaction and questions. Trainers beware: content errors MUST be corrected immediately – wrong content stays in people's heads.

The final wrap-up will take around 15 minutes and also includes asking the groups about the organisational measures they noted down. Discuss these. They could mention: local CERT, users not authorised to install unapproved software, strict and fast patching (and up-to-date antivirus protection) policy, CISO auditing, penetration testing, maintained firewall policy, no personal equipment allowed on corporate LAN.

Use the schema below from the ENISA Good Practice Guide for Incident Management[22] to discuss the potential roles of various parties in improving the incident handling process.

Figure 10: Examples of improvement proposals for parties involved

While the trainer wraps up, the co-trainer finalises the group ratings and writes them next to the ratings of the previous task.

They should be rated according to the following criteria:

- Can they illustrate graphically the infection mechanism?
- Can they explain and answer questions asked by others?
- Can they provide a basic explanation of how to avoid the threat?

30 minutes break.

[22] http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

6 Task 4 – Phishing Role-play: 105 minutes plenary

The trainer gives a 15-minute introduction, which includes time for the groups to read their roles. The trainer explains that the scenario is turning into a role-play, featuring all 7 groups. First the scenario is further developed:

So SUGARLOAF was infected, right, but they did not notice this right away. What happens is that a few days later, SUGARLOAF sees that serious money has left their account in the past few days, with unclear destinations abroad. All employees who deal with CRIBGOCH BANK swear that they did not carry out these transactions, but they did carry out other, valid transactions. These valid transactions can't be found online, however. Something is most definitely wrong. SUGARLOAF's security team, SUGAR-CERT is warned and called into action.

Then the trainer shows a slide with the 7 roles, which stays on display, and the roles are assigned to the groups by the co-trainer handing out the short role descriptions for each group. Meanwhile the trainer explains the rules of the role-play (basically: the trainers have all power, and only ONE person talks at a time) and the roles, making it clear that the countries mentioned are not imaginary (with the exception of Atlantis), but the CERT and organisation names are fictitious:

United Kingdom:

SUGAR-CERT, the CERT of SUGARLOAF

CRIBGOCH IFD (Internet Fraud Division), the CERT of CRIBGOCH BANK

UNION-JACK-CSIRT, the national CERT of the UK

E-CRIME SQUAD, the primary cyber law enforcement team in the UK

MOLOTOV, a commercial security company offering AV tools and research, forensics, vulnerability advisories, etc. – they also have a UK branch office with top-notch experts

Estonia:

EEIRT, the national CERT of Estonia

C-EP (Cyber – Eesti Politsei), the cyber police of Estonia

Atlantis:

Any roles required will be played by the trainers

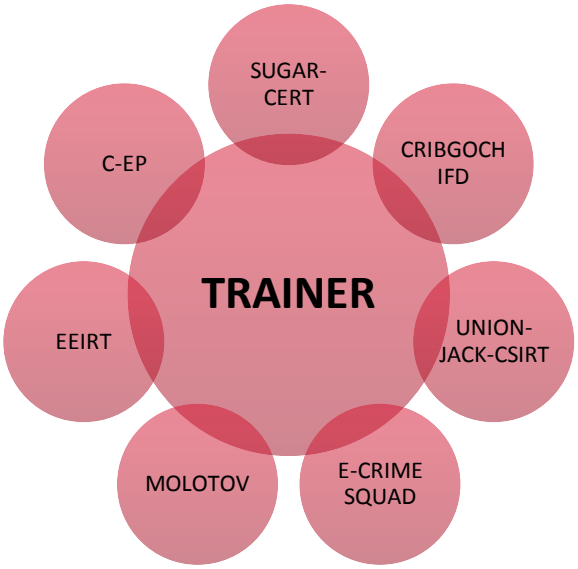


Figure 11: The roles during the role playing and their possible placement

The roles description is the following[23]:

SUGAR-CERT, the CERT of SUGARLOAF. You are the manager of this team. The CERT is quite new to your company and you spent a lot of time convincing people in the company that you needed a CERT. Now is your chance to prove your value, and the company is counting on you because the costs of the phishing attack are quite high. Now is your time to shine.

CRIBGOCH IFD (Internet Fraud Division), the CERT of CRIBGOCH BANK – your team is very mature and you have experienced a lot of phishing in the past. But recently one of your customers blamed the bank for a problem that was undoubtedly his fault. The case became public and hurt the bank's reputation, so now your bosses pay special attention to avoiding such situations.

UNION-JACK-CSIRT, the national CERT of the UK – you are a member of the oldest CERT in the UK. For many years you have been an academic and have been involved with the network without special responsibilities for your constituency. But the situation has changed and now with a grant to act as the national CERT of the UK you have a kind of Service Level Agreement for the British constituency.

E-CRIME SQUAD, the primary cyber law enforcement team in the UK – you are a trained member of the national Police in the UK. Every day you have more and more cases as computer crime is becoming extremely prevalent. Sometimes you are annoyed by the cases, which tend to be almost the same in nature. Today you are even more annoyed as your shift is during a match between the local football team which is playing in the F.A. Cup against Manchester United and you could not find someone to replace you for the day.

MOLOTOV, a commercial security company offering AV tools and research, forensics, vulnerability advisories, etc. – they also have a UK branch office with top-notch experts. You are extremely advanced in investigating phishing cases. Recently you have helped a few banks and you have become recognisable on the market, so there is a significant increase of requests for your service. You have been ordered by your bosses to become picky and take only the most sophisticated cases for good money.

[23] *The descriptions of the roles (ready for cutting out) can be found in Appendix 2.*

EEIRT, the national CERT of Estonia – you are a member of the elite team which was founded a few years ago as a result of massive cyber-attacks on your country. You focus on helping your customers, which include the public administration of the Estonian government and critical information infrastructure operators. Combating phishing is also part of your work but generally you try to stick to Estonian cases only.

C-EP (Cyber – Eesti Politsei), police unit in Estonia, handling cyber-related crime. You try to do your best but in most cases you still have insufficient knowledge about computer crimes.

Note for the trainers: you can use other countries in place of the UK and Estonia, like A and B, if the trainees are mainly from A and B. However any support offered below pertains specifically to the UK and Estonia, so you would need to know what you are doing when you change countries. It would certainly make the exercise more tailored, but be prepared!

After these first 15 minutes when all groups understand the setting and their roles, the trainer kicks off the role-play. The approximate timing for the role-play is 75 minutes, but this depends on how it develops. Internet use is allowed.

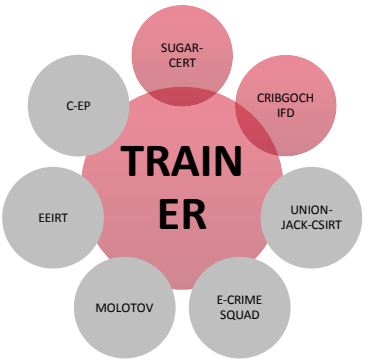
Again, the trainers will rate each group by giving points out of 10 for the most creative **and** accurate role-play – these will be added to the points given before.

The possible criteria could be:

- Involvement in the game.
- Playing a role as described.
- Following the game rules and trainer instructions.

Note: this is **not** a fully free role-play. Make sure that the scenario develops roughly according to the following schema, given in the form of quotes which can mostly be shared with all groups or **even better** in whispers to specific groups only (another option is to hand out a note with the particular addition to relevant players). **But it is preferable for the scenario to develop spontaneously,** and these interjections should be sparse. The text in bold below contains essential information, needed to make this scenario work and involve all parties. [Suggestions for the trainers are between square brackets.] Interject only if you need to revive the game. Generally you should leave an initiative to the players as long as they follow the main parts of the scenario, and step in only if the scenario development goes in a dangerous direction in terms of not fulfilling the game. If you decide to interject make sure that players will be aware of the main actions described in a particular interjection. For this purpose you can use the scenario injects given in Appendix 3.

Inject 1 – SUGAR-CERT phones CRIBGOCH IFD

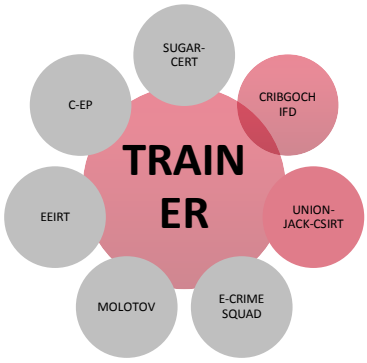


CRIBGOCH IFD soon realises that this may be fraud of an international type. They block the account in communication with SUGAR-CERT and propose that together they get in touch with the national CERT. Also they advise SUGAR-CERT to think about whether they want to involve the police.

SUGAR-CERT asks CRIBGOCH IFD to involve the national CERT – SUGAR-CERT gets in touch with their management [played by a trainer if needed] to think about going to the police. Management is not enthusiastic – they prefer this solved without the police. SUGAR-CERT decides to do what they can to secure evidence anyway, just in case the police might get involved at some stage. [The trainers freeze

the action and ask SUGAR-CERT and the other groups: 'How do you do that?' Internet research allowed.]

Inject 2 – CRIBGOCH IFD phones UNION-JACK-CSIRT



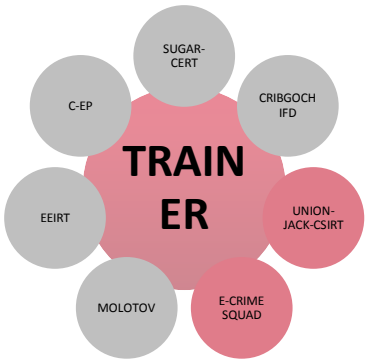
The national CERT suggests involving a security company and/or the cyber police.

CRIBGOCH IFD themselves get in touch with MOLOTOV, one of their regular security providers, and ask them to research.

MOLOTOV gets in touch with SUGAR-CERT and asks if they can come and investigate. SUGAR-CERT agrees, providing that the MOLOTOV people sign an NDA (Non-Disclosure Agreement) when it comes to SUGARLOAF information. [If needed freeze the action to discuss the importance of NDAs under such circumstances.]

MOLOTOV agrees and visits SUGARLOAF. They soon find out that several systems have been infected with a rootkit. ***The installed malware forces systems to use a DNS server in Atlantis instead of the normal one. The DNS server in Atlantis has most likely been hacked by the cyber gang behind this phishing case.*** *It is not directly clear how the attack worked beyond this point, as the Atlantis DNS server seems to be mostly serving the right IP addresses. MOLOTOV suggest letting the systems run without interruption and add a form of 24/7 monitoring.*

Inject 3 – UNION-JACK-CSIRT decides to involve E-CRIME SQUAD

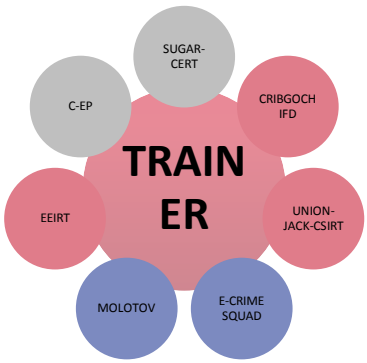


UNION-JACK-CSIRT decides to involve E-CRIME SQUAD anyway, in the background. E-CRIME SQUAD *talks with CRIBGOCH IFD and as a result contacts MOLOTOV. They ask MOLOTOV to secure disk images at SUGARLOAF.*

SUGARLOAF has lost some serious money and it is unclear if CRIBGOCH will compensate this – so management is persuaded to contact the police. [The regular police can be played by one of the trainers. This could be quite interesting as the regular police tend not to be highly cyber aware. Make this clear. Advise to have good contacts with cyber law enforcement.] After some confusion, they get in touch with E-CRIME SQUAD.

The money has gone to several destinations abroad. CRIBGOCH has inquired with the receiving banks, but the money has left the accounts there already for other destinations – the receiving banks refuse to tell where – they will only do that as part of a criminal investigation in their own country. [Freeze action if needed and discuss how complicated cases like these are. And how many parties are needed to resolve them. Ask trainees for their own experiences in this area.]

Inject 4 – MOLOTOV discovers a bad DNS IP. UNION-JACK-CSIRT contacts EEIRT



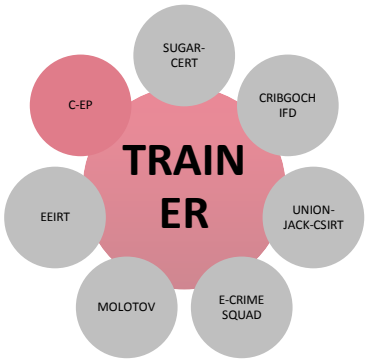
MOLOTOV meanwhile discovers that in the morning, ***the Atlantis DNS server serves a different IP address for CRIBGOCH BANK all of a sudden. The IP address is located in Estonia.*** *MOLOTOV informs E-CRIME SQUAD, UNION-JACK-CSIRT and CRIBGOCH IFD. [Consider forming a virtual team for a case like this, including the major players. Discuss this option. In big crises – this is not a big crisis! – some such people would even sit together, e.g. in the office of the national team.]*

UNION-JACK-CSIRT contacts EEIRT, their colleagues in Estonia. EEIRT is a very effective team who immediately take action. They phone their police colleagues, C-EP. Together they coordinate action.

Meanwhile E-CRIME SQUAD gets in touch with their colleagues in Atlantis. They don't have direct contacts and so they work via Interpol (if needed the trainers can provide this link, plus the Atlantis contact). The Atlantis colleagues are neither interested nor cooperative. If this needs to be pursued it will take a lot of time.

MOLOTOV finds that the Estonian server indeed hosts an emulation of the CRIBGOCH online banking server. Together with the CRIBGOCH team they find that the emulation server acts as man-in-the-middle, thus even 'using' the challenge-response security used by CRIBGOCH to their own advantage. [Freeze action and ask the trainees to explain how this is possible.]

Inject 5 – C-EP does a raid with the company hosting the emulation server



C-EP decides not to lose time and on the basis of the local law they do a raid with the company hosting the emulation server. They secure the disk images.

As this raid disables the emulation server, it is as good a moment as any to stop the action. The case is not closed yet of course, not even close to closed. But we were focusing here on organisational and cyber law (enforcement) issues. And to show how complicated phishing cases like these are – technically, organisationally and legally – and how complex the maze of cooperation soon becomes.

Next, take 15 minutes to discuss the role-play with the trainees, and together take stock of what they have learned.

While the trainer wraps up, the co-trainer finalises the group ratings and writes them next to the ratings of the previous task. All ratings are added up and the winner is revealed. Trainer and co-trainer give the winning group their treat(s).

Ask the groups – what do they do? If the IP address hosts a fake web server for CRIBGOCH BANK, it is more than likely that this is run on an 'owned' server – a hacked server. By just shutting them down, valuable evidence chains might be lost – and besides is it legal to just shut them down? What is the best approach? Discuss.

7 Summary

The most important thing here is to design a wrap-up session based on experiences from the role-playing game. This game includes the most important knowledge about phishing campaign tracking and handling.

You can organise the final discussion using the following questions:

- Was the case realistic?
- What was the difference between the real situation and the one from the scenario?
- What have you learnt from the role playing?
- What could be an improvement plan based on the experience gained from the role-playing game?

8 References

1. ENISA – Protecting Industrial Control Systems – Recommendations for Europe and Member States, 2011 (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states)
2. ENISA – Baseline capabilities for national / governmental CERTs, 2009/2010 (http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities)
3. US-CERT – Recommended Practice: Creating Cyber Forensics Plans for Control Systems (https://www.us-cert.gov/control_systems/practices/Recommended_Practices.html)
4. COUNCIL OF EUROPE – CYBERCRIME LEGISLATION – Country profiles (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/)
5. UNITED NATIONS – The Universal Declaration of Human Rights (http://www.un.org/en/documents/udhr/)
6. WIKIPEDIA – International Humanitarian Law (https://en.wikipedia.org/wiki/International_humanitarian_law)
7. COUNCIL OF EUROPE – Convention on Cybercrime CETS No.: 185 (http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG)
8. SCO SUMMIT 2012 – Official Website (http://www.scosummit2012.org/english/)
9. EUROPEAN COMMISION – Press Release details (http://europa.eu/rapid/press-release_IP-13-94_en.htm)
10. THE JUSTICE AND HOME AFFAIRS COUNCIL – Mutual Legal Assistance Convention, 29-30 May 2000 (http://www.statewatch.org/news/aug00/MLAfinal.htm)
11. EUROPEAN COMMISION – Data retention (http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/index_en.htm)
12. THE EUROPEAN PARLIAMENT AND COUNCIL – Directive 2000/31/EC of, 8 June 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT)
13. EUROPEAN COMMISION – Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA (http://europa.eu/rapid/press-release_MEMO-10-463_en.htm)
14. THE EUROPEAN PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION – Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, December 2011 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF)
15. UNITED NATIONS OFFICE ON DRUGS AND CRIME – United Nations Convention against Transnational Organized Crime and the Protocols Thereto (http://www.unodc.org/unodc/treaties/CTOC/)
16. AGREEMENT on mutual legal assistance between the European Union and the United States of America (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF)
17. EUROPOL – A Collective EU Response to Cybercrime (https://www.europol.europa.eu/ec3)
18. EUROJUST – The European Union's Judicial Cooperation Unit (http://eurojust.europa.eu/Pages/home.aspx)
19. 2CENTRES – European Cybercrime Training & Education Group (ECTEG) (http://www.2centre.eu/europolwg)
20. ENISA – Latest News & Press Releases (http://www.enisa.europa.eu/)
21. ENFSI – Information Technology (http://www.enfsi.eu/about-enfsi/structure/working-groups/information-technology)

22. INTERPOL – Cybercrime (http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime)
23. ERA – Fighting Cybercrime: Between Legislation and Concrete Action (https://www.era.int/cgi-bin/cms?_SID=d0eb0caed658491466aa8c699c4a36ee16f659d900178707229268&_sprache=en&_persistant_variant=/Our%20programme/Browse%20all%20events&_bereich=artikel&_aktion=detail&idartikel=122651)
24. AMERIPOL (http://www.ameripol.org/portalAmeripol/appmanager/portal/desk?_nfpb=false)
25. COUNCIL OF EUROPE – Action against economic crime, About 24/7 Points of contact (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpoc_EN.asp)
26. MICROSOFT (http://cyberlaw.org.uk/wp-content/uploads/2010/02/microsoft-spy.pdf)
27. FACEBOOK – Information for Law Enforcement Authorities (https://www.facebook.com/safety/groups/law/guidelines/)
28. E-BAY – Law Enforcement E-request System (https://lers.corp.ebay.com/AIP/portal/home.do)
29. YAHOO – Compliance Guide For Law Enforcement (http://cryptome.org/isp-spy/yahoo-spy.pdf)
30. ENISA CERT Exercise 'Mobile Incident Handling' (http://www.enisa.europa.eu/activities/cert/support/exercise/files/Mobileincidenthandlinghandbook.pdf)
31. THE PHARMING GUIDE (Part 1, part 2) (http://www.technicalinfo.net/papers/Pharming.html)
32. SYMANTEC – Internet Security Threat Report 2013 (http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf)
33. FRASER HOWARD, SOPHOSLAB – Exploring the Blackhole exploit kit (http://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit/)

9 Appendix 1 – Phishing mail examples

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Figure 12: Phishing mail example 1[24]

[24] http://en.wikipedia.org/wiki/File:PhishingTrustedBank.png

Figure 13: Phishing email example 2[25]

[25] http://howto.cnet.com/8301-11310_39-10396786-285/how-to-recognize-phishing-e-mails/

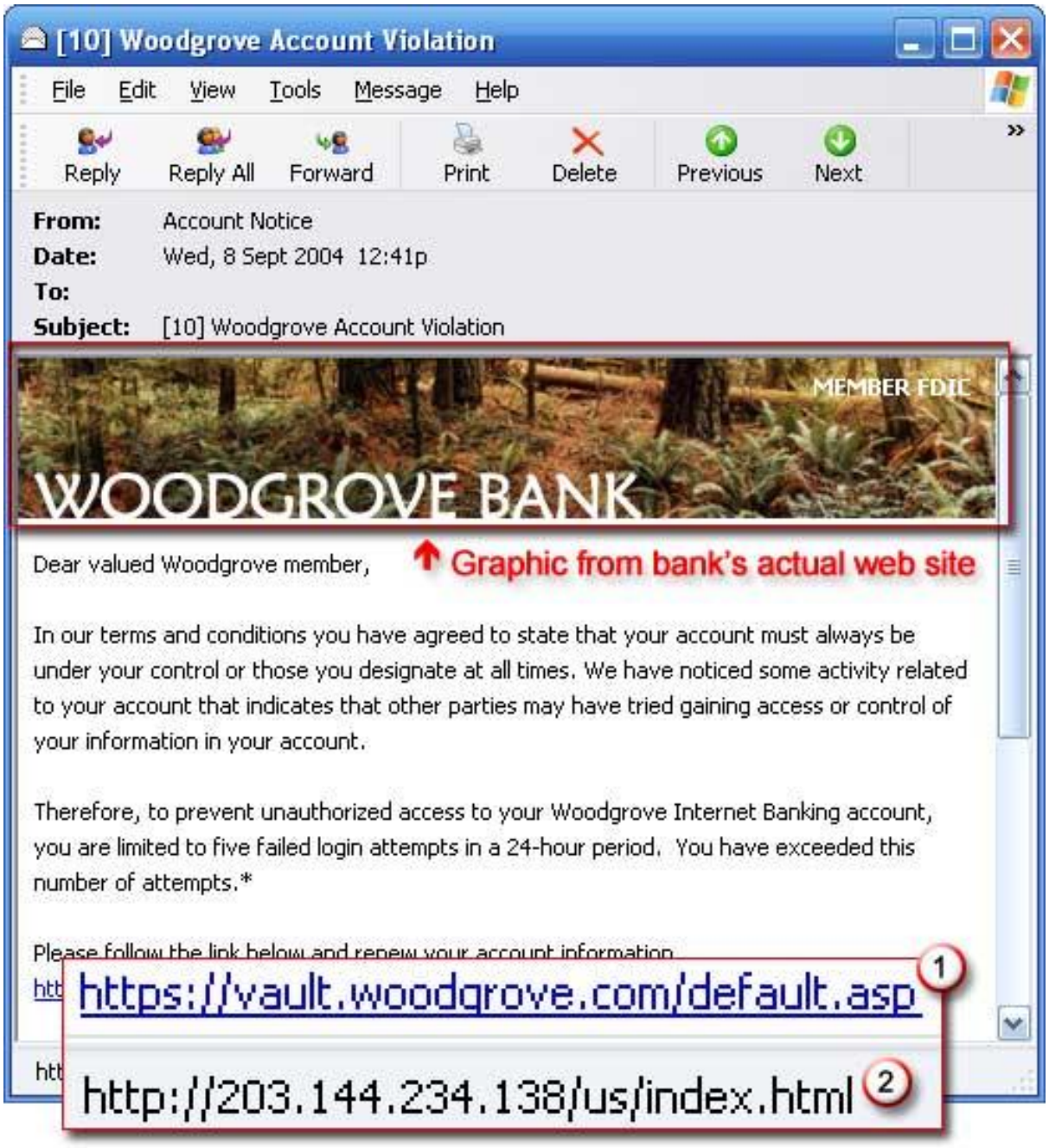


Figure 14: Phishing email example 3

10 Appendix 2 – Roles description

✂ ----------

SUGAR-CERT, the CERT of SUGARLOAF. You are the manager of this team. The CERT is quite new to your company and you spent a lot of time convincing people in the company that you needed a CERT. Now is your chance to prove your value, and the company is counting on you because the costs of the phishing attack are quite high. Now is your time to shine.

✂ ----------

CRIBGOCH IFD (Internet Fraud Division), the CERT of CRIBGOCH BANK – your team is very mature and you have experienced a lot of phishing in the past. But recently one of your customers blamed the bank for a problem that was undoubtedly his fault. The case became public and hurt the bank's reputation, so now your bosses pay special attention to avoiding such situations.

✂ ----------

UNION-JACK-CSIRT, the national CERT of the UK – you are a member of the oldest CERT in the UK. For many years you have been an academic and have been involved with the network without special responsibilities for your constituency. But the situation has changed and now with a grant to act as the national CERT of the UK you have a kind of Service Level Agreement for the British constituency.

✂ ----------

E-CRIME SQUAD, the primary cyber law enforcement team in the UK – you are a trained member of the national Police in the UK. Every day you have more and more cases as computer crime is becoming extremely prevalent. Sometimes you are annoyed by the cases, which tend to be almost the same in nature. Today you are even more annoyed as your shift is during a match between the local football team which is playing in the F.A. Cup against Manchester United and you could not find someone to replace you for the day.

✂ ----------

MOLOTOV, a commercial security company offering AV tools and research, forensics, vulnerability advisories, etc. – they also have a UK branch office with top-notch experts. You are extremely advanced in investigating phishing cases. Recently you have helped a few banks and you have become recognisable on the market, so there is a significant increase of requests for your service. You have been ordered by your bosses to become picky and take only the most sophisticated cases for good money.

✂ ----------

EEIRT, the national CERT of Estonia – you are a member of the elite team which was founded a few years ago as a result of massive cyber-attacks on your country. You focus on helping your customers, which include the public administration of the Estonian government and critical information infrastructure operators. Combating phishing is also part of your work but generally you try to stick to Estonian cases only.

✂ ----------

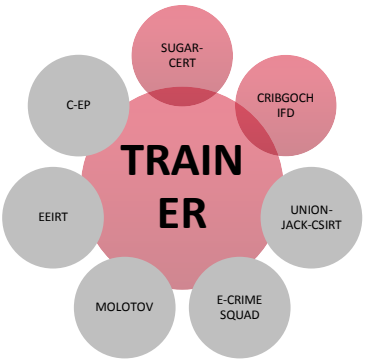
C-EP (Cyber – Eesti Politsei), police unit in Estonia, handling cyber-related crime. You try to do your best but in most cases you still have insufficient knowledge about computer crimes.

11 Appendix 3 – The leaflet of the SUGARLOAF Company

12 Appendix 3 – The role-play scenario injects

✂ ----------

Inject 1 – SUGAR-CERT phones CRIBGOCH IFD

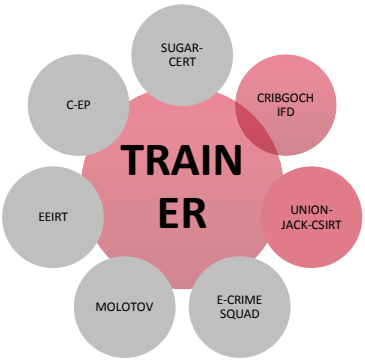


CRIBGOCH IFD soon realises that this may be fraud of an international type. They block the account in communication with SUGAR-CERT and propose that together they get in touch with the national CERT. Also they advise SUGAR-CERT to think about whether they want to involve the police.

SUGAR-CERT asks CRIBGOCH IFD to involve the national CERT – SUGAR-CERT gets in touch with their management to think about going to the police. Management is not enthusiastic – they prefer this solved without the police. SUGAR-CERT decides to do what they can to secure evidence anyway, just in case the police might get involved at some stage.

✂ ----------

Inject 2 – CRIBGOCH IFD phones UNION-JACK-CSIRT



The national CERT suggests involving a security company and/or the cyber police.

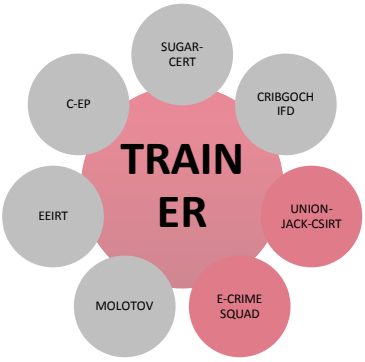
CRIBGOCH IFD themselves get in touch with MOLOTOV, one of their regular security providers, and ask them to research.

MOLOTOV gets in touch with SUGAR-CERT and asks if they can come and investigate. SUGAR-CERT agrees, providing that the MOLOTOV people sign an NDA (Non-Disclosure Agreement) when it comes to SUGARLOAF information.

MOLOTOV agrees and visits SUGARLOAF. They soon find out that several systems have been infected with a rootkit. ***The installed malware causes these systems to use a DNS server in Atlantis instead of the normal one. The DNS server in Atlantis has most likely been hacked by the cyber gang behind this phishing case.*** *It is not directly clear how the attack further worked, as the Atlantis DNS server seems mostly is serving the right IP addresses. MOLOTOV suggest to let the systems run without interruption and add a form of 24/7 monitoring.*

✂ ----------

Inject 3 - UNION-JACK-CSIRT decides to involve E-CRIME SQUAD



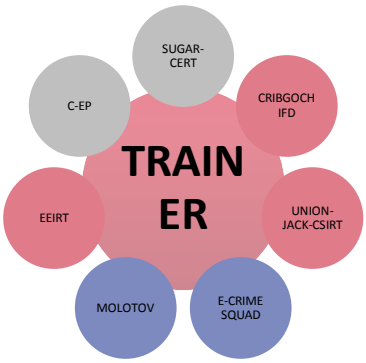
UNION-JACK-CSIRT decides to involve E-CRIME SQUAD anyway, in the background. E-CRIME SQUAD *talks with CRIBGOCH IFD and as a result contacts MOLOTOV. They ask MOLOTOV to secure disk images at SUGARLOAF.*

SUGARLOAF has lost some serious money and it is unclear if CRIBGOCH will compensate this – so management is persuaded to contact the police. After some confusion, they get in touch with E-CRIME SQUAD.

The money has gone to several destinations abroad. CRIBGOCH has inquired with the receiving banks, but the money has left the accounts there already for other destinations – the receiving banks refuse to say where – they will only do that as part of a criminal investigation in their own country.

✂ ----------

Inject 4 – MOLOTOV discovers a bad DNS IP. UNION-JACK-CSIRT contacts EEIRT



MOLOTOV meanwhile discovers that in the morning, ***the Atlantis DNS server serves a different IP address for CRIBGOCH BANK all of a sudden. The IP address is located in Estonia.*** *MOLOTOV informs E-CRIME SQUAD, UNION-JACK-CSIRT and CRIBGOCH IFD.*

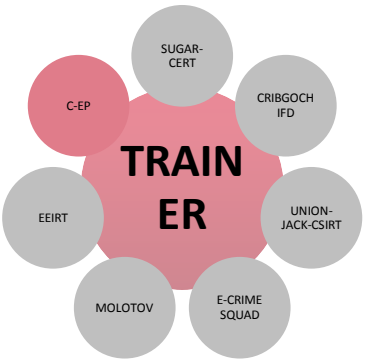
UNION-JACK-CSIRT contacts EEIRT, their colleagues in Estonia. EEIRT is a very effective team who immediately take action. They phone their police colleagues, C-EP. Together they coordinate action.

Meanwhile E-CRIME SQUAD gets in touch with their colleagues in Atlantis. They don't have direct contacts and so they work via Interpol. The Atlantis colleagues are neither interested nor cooperative. If this needs to be pursued it will take a lot of time.

MOLOTOV finds that the Estonian server indeed hosts an emulation of the CRIBGOCH online banking server. Together with the CRIBGOCH team they find that the emulation server acts as man-in-the-middle, thus even 'using' the challenge-response security used by CRIBGOCH to their own advantage.

✂ ----------

Inject 5 – C-EP does a raid with the company hosting the emulation server.



C-EP decides not to lose time and on the basis of the local law they do a raid with the company hosting the emulation server. They secure the disk images.

As this raid disables the emulation server, it is as good a moment as any to stop the action. The case is not closed yet of course, not even close to closed. But we are focusing here on organisational and cyber law (enforcement) issues. And to show how complicated phishing cases like these are – technically, organisationally and legally – and how complex the maze of cooperation soon becomes.

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu