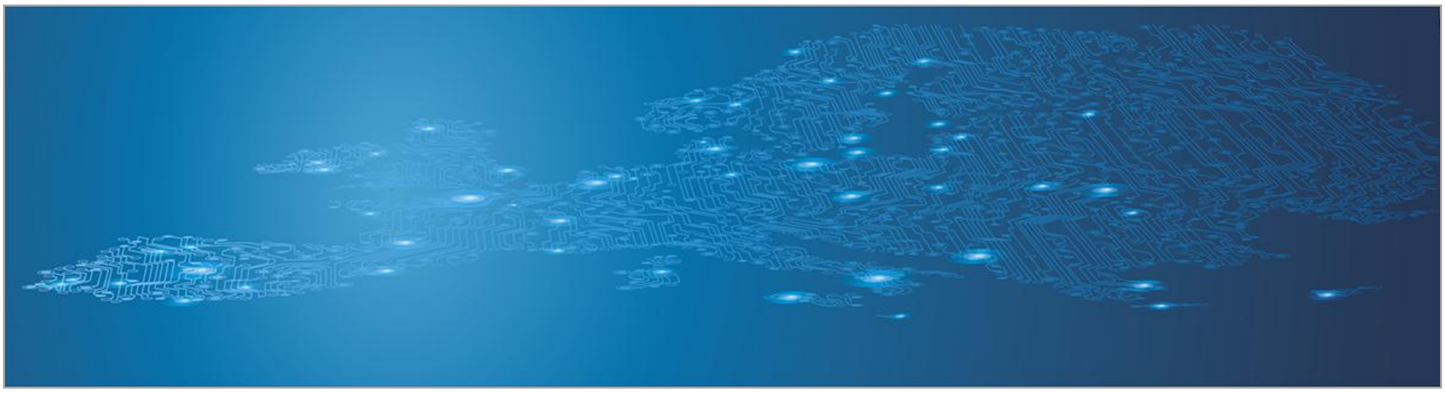


Incident handling and cooperation during phishing campaign

Toolset, Document for students

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 Weżgowiec from ComCERT, Poland, Przemysław Skowron from Poland, Roeland Reijers from Rubicon Projects, The Netherlands and Mirko Wollenberg from DFN-CERT Services, Germany.

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

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

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

Table of Contents

1 What you will learn

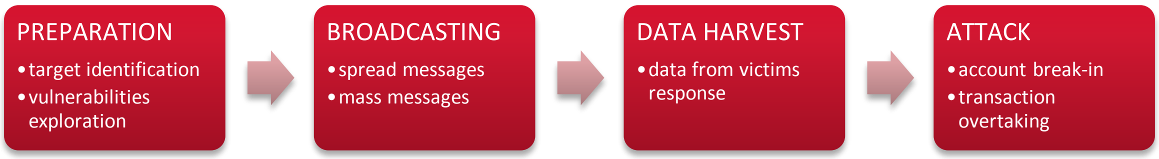
The exercise treats phishing on three levels – moderately technical, organisational and legal. The purpose is to understand phishing campaigns better and how to combat them in complex international contexts.

This exercise is useful for staff of national CERTs, bank CERTs and CERTs for big companies or organisations: all 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.
The goals of the exercise are:

- 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.

2 Introduction

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 its phases as shown in the figure below.



PREPARATION
- target identification
- vulnerabilities exploration

BROADCASTING
- spread messages
- mass messages

DATA HARVEST
- data from victims response

ATTACK
- account break-in
- transaction overtaking

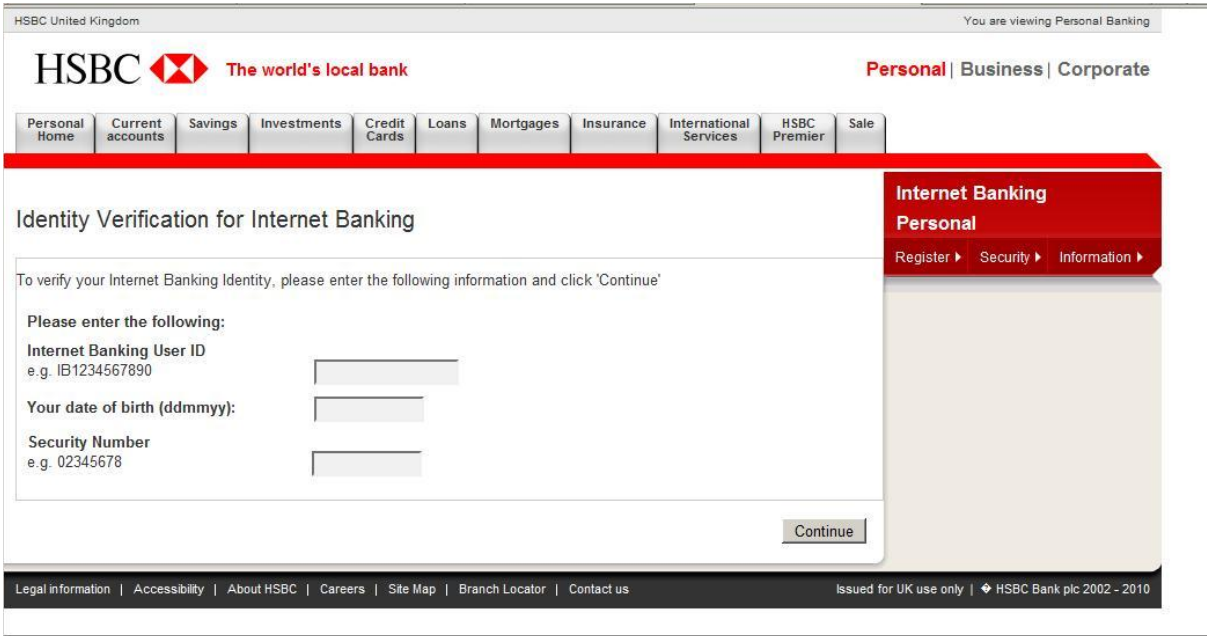
Figure 1: Main phases of phishing attacks

Some background information about phishing:

- *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 charge from 2% of the account balance for US accounts to as much as 6%.
  - 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

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

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.



Identity Verification for Internet Banking

To verify your Internet Banking Identity, please enter the following information and click 'Continue'

Please enter the following:

Internet Banking User ID
e.g. IB1234567890

Your date of birth (ddmmyy):

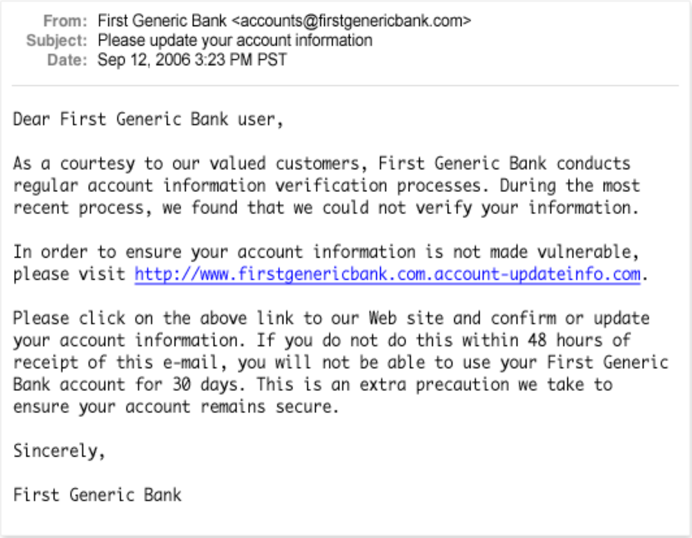
Security Number
e.g. 02345678

Continue

Figure 2: 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 3: An example of a phishing email

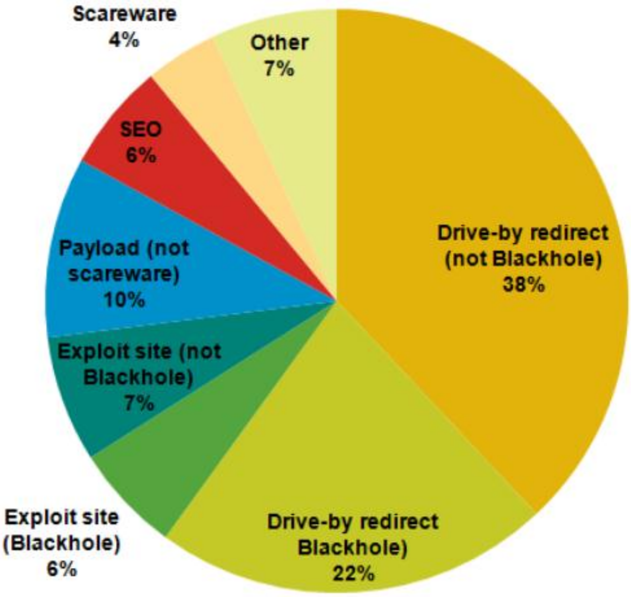


Figure 4: Breakdown of detected web threats by type with the relation to the Blackhole threat. (Source: Sophos Technical Paper: Exploring the Blackhole Exploit Kit[3])

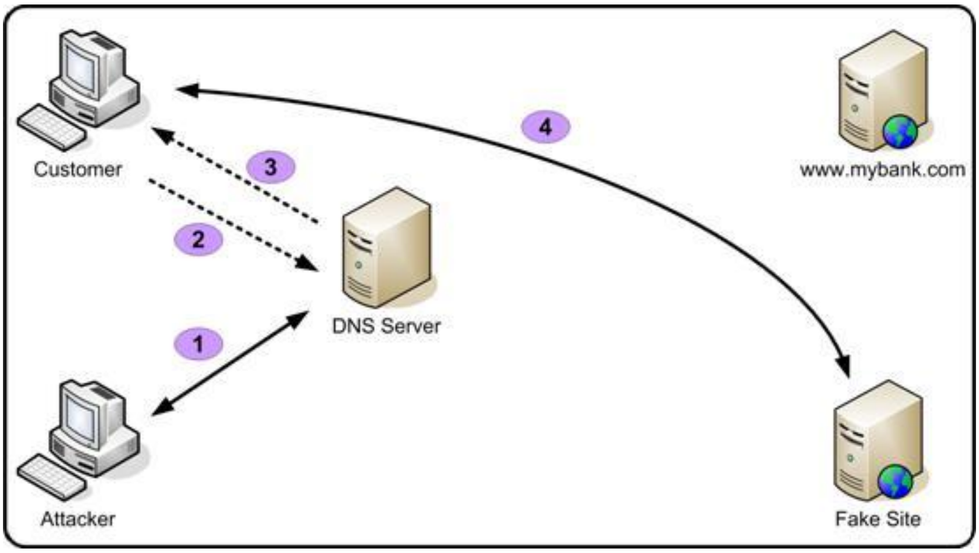


Figure 5: The DNS resolution process having fallen victim to a DNS spoofing attack (source: The Pharming Guide[4])

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 gives a reply and the rogue server sends 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'.[5]

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

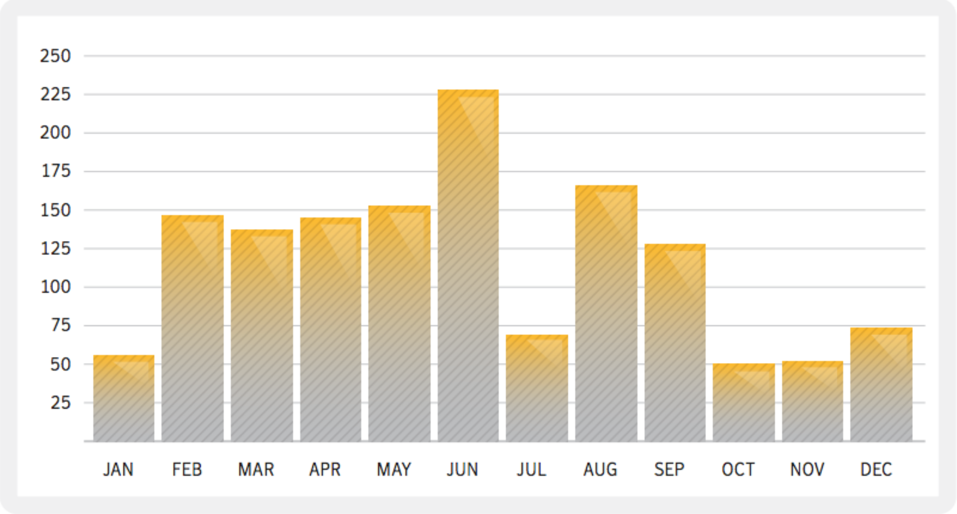


Figure 6: Mobile targeted attacks on clients of the bank organisations per day in 2012[6]

- *Phishing vectors*
  Most popular vectors of infecting user device[7]:
  - 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[8].
  - Mass infection of host service providers became popular in 2012[9] – 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.[10] 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.
- *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[11] – the trainer is advised to read the short article referenced.

[6] *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*
[7] *According to authors and contributors recommendations and observations*
[8] *http://arstechnica.com/security/2013/07/darkleech-infects-40k-apache-site-addresses/*
[9] *http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2012.pdf*
[10] *http://arstechnica.com/security/2013/05/attack-hitting-apache-sites-goes-mainstream-hacks-nginx-lighttpd-too/*
[11] *http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year*

3 Exercise Tasks

You are allowed to use laptops or handhelds to connect with the Internet during the exercise, whenever this supports the exercise. The trainer will make clear when and how. Please remember that the use of computers and the Internet is meant as fall-back and background activity, as the main activities should be carried out together with your fellow trainees!

3.1 Task 1 – Phishing Messages

The scenario that is used throughout this exercise is kicked off (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.*

SUGARLOAF TRADING UK Ltd.
SUGARLOAF
Company News
Cardiff – the new docks opened
Containers ready for shipping
SUGARLOF CEO says – "Our sweet customers are the most important"
New partner in business – CRIBGOCH BANK
SUGAR everywHERE
CARDIFF
GDANSK
AMSTERDAM
TALLIN
HERAKLION
HAMBURG
HAVANA
SYDNEY
BOSTON

Figure 7: The Sugarloaf Company leaflet

> *A spear phishing attack is targeted at several branch offices of the shipping company SUGARLOAF TRADING in the UK. The phishing attack 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)*

Each group will do the following:

(1) Devise the most clever phishing email you can think of in the context described. The message really needs to convince employees of SUGARLOAF to do whatever the phishers want them to do in order to get infected. Write this message down.

(2) Briefly describe what infection mechanism is inherent or invoked in your phishing email, i.e. how the infection would take place and what malware might be involved.

(3) Finally, you need to describe briefly:

- 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 – and similar – attacks from being successful

30 minutes in groups, ready, go. Internet use **not** allowed

3.2 Task 2 – Infection Mechanisms

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.*

Each group will do the following:

(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, you need 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,[12] 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)

30 minutes in groups, ready, go. Internet use necessary.

3.3 Task 4 – Phishing Role-play

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.*

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

These are the role-play roles (each role/group will receive role details separately):

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

4 Summary

By the end of this exercise, you should 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.

5 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 Humans 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 – 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 Erequest 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/)

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