ANTI-PHISHING POLICY

APRIL 2020

CONTENTS

1 Overview

The National Cyber Security Centre (NCSC) describe Phishing as (Ref [1]):

"Phishing describes a type of social engineering where attackers influence users to do 'the wrong thing', such as disclosing information or clicking a bad link. Phishing can be conducted via a text message, social media, or by phone, but these days most people use the term 'phishing' to describe attacks that arrive by email. Email is an ideal delivery method for phishing attacks as it can reach users directly and hide amongst the huge number of benign emails that busy users receive"

Phishing attempts can be generic and delivered en masse or highly targeted to an organisation or an individual and in the modern day, Phishing is one of the most prevalent attack vectors due to its simplicity, speed and the value of the information that can be extracted in this manner.

Since Phishing generally plays on human nature to be successful, it ultimately relies on user recognition and training to mitigate the risks. This makes mitigation of Phishing attacks non-trivial to mitigate in large organisations and therefore Phishing success rates are high, making this an area of significant importance within IL7 to investigate and control.

1.1 Purpose

This document provides interim guidance to IL7 on how to mitigate the risks from Phishing attacks that can be used when developing systems, implementing anti-phishing controls and advising staff on how to recognise and respond to phishing attempts.

Future Policy will provide requirements that IL7 systems and users must meet.

1.2 Scope

This interim policy primarily focusses on mitigating the risks from Phishing via email although some is more generally applicable. Future policy will also cover other forms of phishing, for example via SMS and Phone calls.

1.3 Applicability

This policy applies to all IL7 staff, service providers and contractors who use systems to support IL7.

2 Anti-Phishing Policy

When designing a system, there are several technical controls that are required to be implemented to mitigate the risk from Phishing attacks. These are detailed in this section and are broadly broken down into three sections:

1. Email Security;
2. Boundary Security;
3. Server and Client Security.

This guidance should be read in conjunction with existing cyber security policies.

Policy ID	Policy Requirement
1	Where emails are received from any domain external to IL7, consideration should be given to automatically tagging the subject line and/or email body text with “[EXTERNAL]” to highlight to users that the email has arrived from an external source.
2	Where emails are received from a domain trusted by IL7 but not internal to IL7, for example other government departments, consideration should be given to automatically tagging the subject line and/or email body with text to highlight to users that the email has arrived from an external, but trusted domain. This should be a different warning from that of 1 so as to highlight if a trusted external domain is being spoofed.
3	Where emails are received from external sources, the user should be provided with the ability to report Phishing emails to a Phishing Reporting Centre or Incident Management Team through a simple process (for example a Phishing reporting email inbox).
4	Hyperlinks received via email should be automatically expanded to present the whole link to the recipient rather than user generated text.
5	When following hyperlinks in emails to external domains, users should be presented with a warning message highlighting that they are visiting an external website.
6	Where possible, documents containing macros should be blocked by the email system with the exception of those documents containing macros signed by IL7 macro signing team.
7	Transport Layer Security (TLS) should be enabled by default to protect emails in transit. See Reference [2] for implementation guidance.
8	Configure Domain-based Message Authentication, Reporting and Conformance (DMARC) on the domain. See Reference [2] for implementation guidance.
9	Configure Sender Policy Framework (SPF) on the domain. See Reference [2] for implementation guidance.

10	Configure Domain-Keys Identified Mail (DKIM) on the domain. See Reference [2] for implementation guidance.
11	System owners must register with NCSC's Mail Check service to identify weaknesses in and monitoring of email services. See Reference [3] details.
12	Emails internal to IL7 should be digitally signed to ensure authenticity within the domain.

3 Boundary Security

Where a IL7 email service interfaces with external domains, at the network or logical boundary to an external system, the following must be implemented.

Policy ID	Policy Requirement
13	All emails and attachments must have anti-virus and malware checks at the boundary to IL7 systems, from a different AV supplier than that used internally on clients.
14	Deep content inspection of attachments should take place to recognise the true file type
15	Emails containing executable, compressed (that cannot be uncompressed and scanned) or password protected attachments (that cannot be opened for scanning) must be blocked at the boundary to IL7 systems.
16	Emails from known spam/bad domains must be dropped at the boundary.
17	Where possible, adaptive redaction of emails should take place, to remove credit card details and other sensitive information that users may unwittingly release. This should also be used to remove known links to websites known to host malicious software or relating to previous phishing messages.
18	Protective Monitoring of emails crossing the boundaries that identifies suspicious patterns of activity (e.g. a user sending out a large number of emails in a short timeframe) in line with IL7 Protective Monitoring Policy (in development).
19	The internet boundary must block access to websites known to host malicious software or known to be related to previous phishing messages.
20	Where hyperlinks are present within emails, these must be tested by the email boundary service in a sandbox to detect malicious activity before being delivered to the user.

21 Server and Client Security

To protect against the impact of malicious email servers and clients should be configured such that:

Policy ID	Policy Requirement
22	Accounts with administration privileges do not have access to email inboxes.
23	Malware protection in line with IL7 Malicious Code Protection Policy (Ref [4]) is installed and kept up to date.
24	Software is regularly patched in line with IL7 Software Maintenance Policy (Ref [5]).
25	User privileges are kept to the minimum required for their role – users should not be able to run executable code except when explicitly authorised by the system (e.g. through the use of AppLocker).
26	Should a user attempt to navigate to a site known to be in use for phishing this navigation should be blocked by the browser and a warning displayed.
27	Activity on the server or client is protectively monitored in line with IL7 Protective Monitoring Policy (in development).

4 Procedural and Personnel Controls

While technical controls can reduce the number of phishing emails encountered by system users it is highly unlikely that these controls can remove all risk of users receiving such emails. As such, it is recommended that all staff using a system are trained to detect phishing emails in line with the guidance in this section and that they understand how to report the receipt of a phishing email.

5 Training Requirements

All users of a system must receive training (in line with NCSC guidance (Ref [1])) that:

Policy ID	Policy Requirement
28	Encourages users to seek help on receipt of a suspected phishing message or if they suspect they may have fallen for a phishing message.
29	Educates users on how to report a suspected phishing message.
30	Reminds users that they will not be punished for reporting a phishing message or for not recognising a phishing message prior to clicking on a link/entering their details etc.
31	Teaches users to look out for 'urgency' or 'authority' cues that pressure the user to act (as discussed in CPNI's 'Don't take the bait' campaign (Ref [6])).
32	Ensures that users are familiar with processes that might involve email communication to empower them to recognise unusual requests.
33	Trains users using real-world examples.
34	Includes, where appropriate, a phishing exercise/workshop for users on the live system.
35	Teaches users to understand the impact of information shared on their own social media pages.

6 Incident Response

Where a suspicious message is received users should:

Policy ID	Policy Requirement
36	Be given a simple means to report that message to the CSOC team (preferably via a single link on their homepage).
37	Have access to a secondary means of communicating a suspicious message in case their system is compromised (e.g. via telephone).
38	Be kept informed of action being taken in response to their report
39	Not be punished for reporting when they believe they may have fallen for a phishing message but encouraged to seek further advice.
40	Be encouraged to seek further guidance where they have fallen for a phishing message to help reduce this risk in the future.
41	Where relevant, have new login information generated for them and be advised to follow the password reset process for the system affected.

7 Exemptions, Exceptions and Breaches

7.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, please refer to the exemptions and exceptions policy (Ref [7])

7.2 Breach of Policy

IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in IL7 Disciplinary Procedure.

Breaches of this Policy by a third party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third party service provider and/or the cancellation of any contract(s) between IL7 and the third party service provider.

IL7 will refer any use of its IT resources for illegal activities to the Police.