Incident Response Action Card Phishing

Version:1

22 December 2022

1 Scope

1.1 This document applies whenever the security of an ICT system or data is impacted, or has the potential to be impacted, by a malicious phishing threat.

1.2 The action card is intended for use by operational officers, primarily within ICT and [response] teams. All ICT individuals who participate within incident response can adopt and use this action card where appropriate.

1.3 The guidance in this action card expands on and must be read in conjunction with the internal Council Cyber Security Incident Processes and Procedures. Adherence to guidance within both documents is required for effective Incident Response.

1.4 Any contractual, legal or government regulatory requirements mandating more stringent requirements than specified in this action card will supersede the requirements of this document.

2 Baseline Recommendations

2.1 **Retain a full audit trail of your actions** in order to avoid problems in a criminal case.

2.2 **Implement the Triage phase** immediately wherever possible.

2.3 **Implement the Triage and Contain phases** swiftly in order to avoid further criminal damage including system breaches and data loss.

2.4 **Process assets individually through phases** in order to avoid undue delays which increase the incident severity – i.e. do not wait for full information before taking action.

2.5 **Implement the Analysis and Search phases comprehensively** in order to avoid persistent criminal presence within Council systems.

2.6 **Defer the Recovery phase until the Isolate phase is complete** in order to avoid persistent criminal presence within Council systems.

2.7 **Regularly update [incident coordinator] on situation** in order to avoid undue delays which cause the Council to breach legal requirements.

What should you do, if a suspected phishing threat is reported/uncovered?

Phase	Action
Immediate *Triage*	**Aim-** *Record the incident details and obstruct obvious threats.* 1.1 **Obtain incident details from the customer:** • Full description, impact and scope. • Physical and logical locations including [asset]. • Customer names and [account names]. • Email: From, To, Date, Subject and Body fields. • Whether a user clicked a hyperlink and which one. • Onscreen messages. • LAN and internet applications with a user login. • Record outcomes of actions above. 1.2 Secure suspect software for analysis. • Send [email sample] to [response officers]. • Delete suspicious email on user device. ⚠ **[malware samples] are unsafe and should be handled with extreme care.** **If at this point if a potential compromise is suspected:** 1.3 Obstruct any clearly identified threats and preserve evidence for analysis: • **Disconnect endpoint network cable & wireless.** • **Disable customer [accounts].** • Change customer [credentials]. • Disconnect the power cable. • Instruct the customer to leave the endpoint and all peripherals unused until further notice. • Ask the customer to place a notice on the device prohibiting usage with [incident reference number]. • Record outcomes of actions above. ⚠ **Do not remotely connect to a suspect device as this may compromise [admin systems].** ⚠ **Do not initiate a PC shutdown as this may interfere with criminal evidence.** 1.4 Obstruct any clear extended threats: • Log a new [request] for credential changes. • Change customer LAN application credentials. • Change customer internet application credentials. • Record outcomes of actions above. ⚠ **Do not send any new customer credentials via email.** 1.5 Notify the [governance officers]. 1.6 Notify the [security officers].

<table>
<tr>
<td>Identify
Analysis</td>
<td>
Aim: Quantify the threat and compromise indicators in detail.
<table>
<tr><td>2.1 Subject malware/hyperlinks to analysis:
Samples for security providers.
Resources: [security systems].
⚠ Only use safe malware handling methods. [INSERT COUNCIL SPECIFIC INFO]</td></tr>
<tr><td>2.2 Confirm incident details and any false-positives with the customer and ICT colleagues.</td></tr>
<tr><td>2.3 Determine attack details:
Email sender, domains, IP addresses.
Malicious web sites, IP addresses.
Compromised assets: accounts, devices, systems.
Assets at risk: accounts, devices, systems.
Number of affected assets and rate of increase.
Entry and exit communications.
Stolen email data.
Suspicious activity in central logs.
Resources: [security systems].</td></tr>
<tr><td>2.4 Review threat intelligence including [intel sources].</td></tr>
</table>
If at this point a potential compromise is suspected:
<table>
<tr><td>2.5 Determine data loss:
Review central logs for unauthorised access.
Review central logs for data loss.
Review central logs for onward spread between endpoint devices.
Resources: [security systems].</td></tr>
<tr><td>2.6 Determine detailed compromise indicators:
Consult security providers.
Resources: [security systems].</td></tr>
<tr><td>2.7 Contract forensic consultancy and analysis.
⚠ Only use safe malware handling methods. [INSERT COUNCIL SPECIFIC INFO]</td></tr>
</table>
</td>
</tr>
<tr>
<td>Identify
Search</td>
<td>
Aim: Reveal the full extent of any malicious compromise.
⚠ If incident severity is increasing, then notify [security team] immediately

If at this point a potential compromise is suspected:
<table>
<tr><td>3.1 Search for malicious intrusion or malware:
Review network and anti-intrusion systems.
Resources: [security systems].</td></tr>
<tr><td>3.2 Search mailboxes for phishing emails:
Emails and attachments opened, or links clicked.
Resources: [security systems].</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td>Contain
Isolate</td>
<td>Aim: Assert control in order to limit exposure to the threat.
⚠ If threat is contained or uncontrollable, then continue to Erase phase.

If at this point a potential compromise is suspected:
<table>
<tr><td>4.1 Neutralise the attack, telemetry and data loss:
Firewalls and switch ports.
Anti-intrusion and proxy systems.
Remote mobile endpoint deactivation.
Resources: [security systems].</td></tr>
<tr><td>4.2 Block onward transmission between endpoints:
Quarantine zone firewalls and switch ports.
Anti-intrusion systems.
Remote mobile endpoint deactivation.
Resources: [security systems].</td></tr>
<tr><td>4.3 Quarantine affected endpoints:
Seize suspect endpoints and peripherals.
Securely transport and store suspect devices at [security office].
⚠ Maintain strict audit trail for legal evidence.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Remove
Erase</td>
<td>Aim: Neutralise or destroy the threat.
⚠ If Erase infects new devices, then revert to Search and Isolate phases.

If at this point a potential compromise is suspected:
<table>
<tr><td>5.1 Obtain erasure guidance from security providers.
Resources: [security systems].</td></tr>
<tr><td>5.2 Scan and disinfect/delete malware:
Emails, attachments, documents and files.
Resources: [security systems].
⚠ Only use read-only media on infected devices. Malware must not be allowed to spread outside the quarantined zone to infect clean devices.</td></tr>
<tr><td>5.3 Delete compromised assets:
[accounts] including profiles.
Operating systems and firmware.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Remove</td>
<td>Aim: Facilitate a return to normal business.
⚠ If Recover spreads the threat, then revert to Search and Isolate phases.

If at this point a potential compromise is still suspected:
<table>
<tr><td>6.1 Allow legitimate network traffic:
Quarantine zone, firewalls and switch ports.
Anti-intrusion and proxy systems.
Resources: [security systems].</td></tr>
</table>
</td>
</tr>
</table>

Recover	6.2 Allow legitimate software processes: • Operating systems and application control. • Resources: [security systems].
	6.3 Replace [accounts]: • Strong credentials and mailbox. • Home and other folders. ⚠ **Do NOT reuse compromised [accounts].**
	6.4 Replace endpoint devices: • Issue new devices and peripherals. Instruct the customer NOT to reuse passwords.
	6.5 Complete vulnerability scanning of all systems, across the estate.
Post-Incident	6.6 Conduct further root-cause analysis to identify and remediate underlying vulnerabilities.
	6.7 Draft a post-incident report that includes the following details as a minimum: • Details of the cyber incident identified and remediated across the network to include timings, type and location of incident as well as the effect on users; • Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed; • Recommendations where any aspects of people, process or technology could be improved across the organisation to help prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process.
	6.8 Complete the formal lessons identified process to feedback into future preparation activities.

How and where to externally report a Phishing Incident:

Activities may include, but are not limited to:

- No matter how severe, you should report the incident to the NCSC, this can be done through the 24hr a day reporting service https://www.ncsc.gov.uk/section/about-this-website/contact-us.
- If you have been subject to or there is evidence of a data breach, you are required to report this under the GDPR, please contact the ICO (Information Commissioner's Office) within 72 hours of becoming aware of the breach, where feasible. https://ico.org.uk/for-organisations/report-a-breach/ . You don't have to wait for 72 hours in theory – the sooner you contact the ICO, the better.
- If there is evidence of fraud or cybercrime, please refer to the **Action Fraud website**.
- Report, if appropriate to peer sharing groups such as your Warning Advice and Reporting (WARP) for onward sharing.

Where can you access related information:

- NCSC's 'Defending your organisation against phishing'- https://www.ncsc.gov.uk/guidance/phishing
- NCSC's 'Phishing Reporting Service'- https://www.ncsc.gov.uk/information/report-suspicious-emails

Related guidance:

Scottish Government Incident Response Guidance and Playbooks- https://www.gov.scot/publications/cyber-resilience-incident-management/

NCSC Incident Management Guidance: https://www.ncsc.gov.uk/section/about-ncsc/incident-management

NCSC CIR (Computer Incident Response) approved companies: https://www.ncsc.gov.uk/information/cir-cyber-incident-response

NCSC Cyber Aware Campaign: https://www.ncsc.gov.uk/cyberaware/home

Attribution:

Jonathan Reed- Hull City Council