Tertiary Education Commission
Te Amorangi Mātauranga Matua

Phishing Response Guidance

How to prepare and respond

Phishing Response Guidance

This guidance is to help your organisation respond to a phishing email to reduce its impact on your business as much as possible. We're outlining what steps to take based on how critical the situation is.

Because preparation is key to readiness and resilience, we're helping you to tackle some important early considerations, like roles and responsibilities. We then cover what to do after an event.

We've also included some valuable resources, like further advice and templates, so you can make sure you have the right tools ready to go.

Before

Preparation is key to readiness and resilience. Make sure your organisation is ready to respond to a phishing attack ahead of time:

› Educate staff so they can recognise a phishing email and know who to go to if they come across one.

› Have a communications approach ready that explains how you will communicate with staff, customers and the public.

› Have the right people in place, doing the right things, at the right time.

IMPORTANT: Where there are actions required that your organisation cannot do on its own, look to engage a security partner to make sure you can take these critical steps.

Put the right people in the right places

It's important to define roles and responsibilities early on. One person may be designated to take charge of all the responsibilities in an event – like an IT person or business manager. Or there may be a leader or coordinator who delegates responsibilities across the business. Ensure these roles are covered:

› Response coordinator: This role leads the incident response. Anyone can take on this role except for your incident investigator, who must focus on investigating the incident.

› Incident investigator: This role requires technical expertise to investigate and contain the issue, before taking measures to stop it happening again in future. If it's a complex issue, you might need several people to investigate – or to engage a security partner.

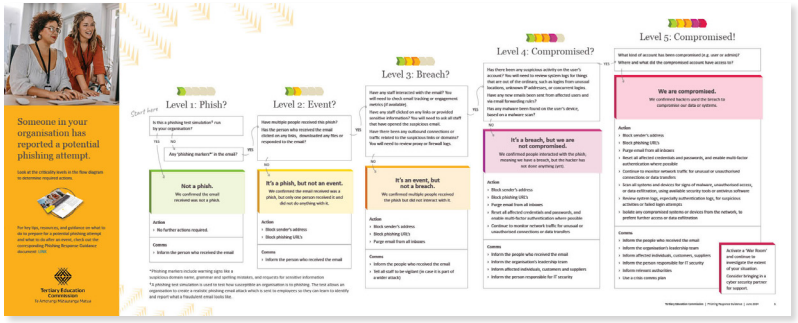
› Staff communicator: This role keeps impacted staff up to date as the incident progresses.

› External communicator: This role manages the crisis communications plan, affected customers, shareholders and media as required. You may want to engage an external communications specialist for this role.

› Manager of business-as-usual: This role ensures business continuity. Even if your IT systems are unavailable, or under the control of an attacker, keep operating to reduce the impact on your business.

During

If you suspect a phishing attempt has occurred, refer to the corresponding phishing response guidance flow diagram. We've outlined what steps you should take based on how critical your situation is.



https://www.tec.govt.nz/assets/Forms-templates-and-guides/CSTS/Controls/TEC-phishing-guidance-poster.pdf

After

Consider what you can learn from an event:

- You may want to hold a post-incident review/debriefing, especially if the incident was large scale.
- Incorporate lessons learnt to create better processes and a stronger organisation.
- It's a good idea to run through a practise scenario every six months to help refine your processes and keep your staff up to speed, as well as to update your contact list, roles and/or policies.

Key Tips

Preparing for the impact of a phishing incident

To protect your organisation from serious damage this guidance focuses on a fast and effective response to an incident. However, it's vital to prepare for a situation where a phishing attack is successful, and your business is hit hard.

You should:

› Identify your business' most important functions. How will you make sure you can keep doing these things if you're compromised?

› Identify critical technology. How will you operate without this? For example, if your email is down.

› Check if your critical data is backed up. Can you restore this data if needed?

Preparing for other types of attack

This guidance focuses on responding to a phishing email. However, other types of attack can benefit from a similar response. For example:

› **Smishing (SMS Phishing):** This involves fraudulent text messages (SMS) that attempt to trick the recipient into revealing sensitive information or clicking on malicious links. The messages often impersonate legitimate organisations or authorities.

› **Vishing (Voice Phishing):** In vishing attacks, the attacker uses phone calls or voice messages to impersonate a trusted entity and manipulate the victim into revealing confidential information or taking a specific action.

› **QRishing (QR Code Phishing):** This involves embedding malicious links or malware within QR codes that don't seem out of the ordinary. When an unsuspecting victim scans the QR code with their mobile device, the device could become infected with malware, or the victim may be redirected to a malicious website designed to steal their credentials or personal information.

Resources

- The National Cyber Security Centre has valuable guidance on incident management, including how to develop an Incident Management Plan: https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Incident-Management-Be-Resilient-Be-Prepared.pdf
- Own Your Online offers simple steps to help you evaluate how an incident could affect your business and how to create a plan: https://www.ownyouronline.govt.nz/business/get-protected/guides/create-an-incident-response-plan
- AlertMedia covers how a crisis communications plan supports emergency management in seven comprehensive steps: https://www.alertmedia.com/blog/crisis-communication
- The Community Comms Collective has a raft of resources and tools to help you with cyber-security communications activities – including internal communications, media relations and reputation management: https://communitycomms.org.nz/resources
- Phriendly Phishing tells you how to recognise a phishing scam: https://www.phriendlyphishing.com/blog/what-is-phishing
- If you have a breach, notify CERT NZ: https://www.ownyouronline.govt.nz/contact-us
- This guidance is a starting point for your organisation to develop its own Incident Management Plan. There are many templates available, for example this one from the Victoria Government: VicGov-Cyber-Incident-Response-Plan-template.docx (live.com)