Cyber incident response toolkit

It is a sad reality that, no matter who you are, you are likely to experience a cyber attack at some point in your life. All individuals and organisations are vulnerable.

You probably have a plan for dealing with issues like natural disasters. As with any crisis, being prepared for an attack and knowing how to respond can save your organisation.

A cyber incident response plan will help you to limit the damage of an attack, get the right people involved to solve the problem, communicate effectively with everyone affected, and prevent further attacks.

This toolkit has three parts:

1. What to do if there is a cyber incident – a four-step guide
2. A classification of common cyber threats
3. A cyber incident response plan template

Use this toolkit as a guide to help your organisation develop your own response plan.

A small business will have a very different plan from a large government department and not everything in this toolkit will feel relevant to you. So, it is important that you develop the plan that will work for you and your organisation. Talk about it, write it all down, and make sure that everyone knows the plan and has access to it – we recommend keeping a hard copy in a safe place, so you can access it even if your devices aren't working.

What to do if there is a cyber incident

1 Identify a cyber attack

You may notice:

- Your passwords aren't working, or you can't access your usual accounts, files or programs
- Unauthorised money has been taken out of a bank account
- Your website isn't working or has been replaced with other content
- You receive a threat or demand to pay a ransom
- People say you sent them a strange email
- Your devices are just being weird – slower than usual, settings are different, there are pop-ups, or files are missing.

See the Common cyber threats document for more information.

2 Control the incident

Get the support you need

Tell your IT expert and gather your cyber incident response team – if you don't have an IT specialist in your organisation, you might need to call for external help.

You may also need to inform:

- The police
- Your organisation's bank, internet provider and insurance company
- Your local Computer/Cyber Emergency Response Team (CERT).

Minimise the damage

Work with your incident response team or IT support to remove the threat and minimise the damage.

- Contact your bank to block any unauthorised payments.
- Don't engage with scammers or cyber criminals.
- Don't use accounts or software that might be compromised until your IT expert says it's okay.
- Contact any staff, suppliers, customers or others in your network that might be affected.
- Change your passwords.

Your organisation's Cyber Incident Response Plan should include more information on who needs to be notified and how, who to go to for help, and communicating with the media and other stakeholders.

3 Get back online, securely

Work with your incident response team or IT support to get back online. This might include downloading new software, restoring backups and scanning for viruses.

4 Learn for the future

Conduct a post-incident review to learn how to better protect yourself in the future. Make any necessary changes to your cyber security and incident response processes and provide staff training so you're prepared next time there is an incident.

Common cyber threats

Threat/incident	What does it look like? (Symptoms)	What to do
Denial-of-Service (DoS) attack: Stops people from accessing your website by flooding it with more fake users than it can handle or redirecting people away from it.	• Files or websites taking an unusually long time to load • You can't load your organisation's website or any website • Unusually high number of visitors to your website.	1. Ask your service providers for support, such as your internet provider or the company that hosts your website. 2. Contact an IT or cyber security expert for help with a denial-of-service attack mitigation service.
Phishing: Tricks people into giving over private information or clicking on dodgy links.	• Suspicious emails and messages • Unexpected bank account activity or signs of malware might mean that someone in your organisation has fallen for a phishing scam	1. If you spot a phishing scam attempt, don't click on any links or download any attachments, and block and report the sender. 2. If you or someone in your organisation has fallen for a phishing scam, check for signs of malware or other threats and follow steps to recover. 3. Contact your bank and other service providers to check your accounts are secure. 4. Make sure your device is clean of malware and then change your passwords. 5. Let your coworkers know to watch out for similar attempts.
Malware: Dangerous software that travels like a virus through the internet to harm your devices or network.	• Your passwords aren't working or you can't access your usual accounts, files or programs • Your device is slow, keeps overheating or is running out of battery faster than usual • Unexpected files or programs installed on your device • Error messages or pop-up ads.	1. If there is unusual activity on your accounts, contact your bank and other service providers to block unauthorised payments and access (see account compromise). 2. Avoid entering passwords if your device is infected with malware. 3. For laptops and computers, disconnect from all networks and other devices, and use your anti-virus software to scan, detect and remove malware. 4. For phones and tablets, back up important files to a cloud service and perform a factory reset on the device to remove malware, then restore from your backup. 5. Change your passwords. 6. Keep an eye out for other suspicious activity.
Ransomware: A type of malware that locks you out of your files or devices, or steals and then threatens to leak sensitive information, unless you pay a fee.	• There are signs of malware like you can't find or access accounts, files or devices • File names have been changed • You receive a message – as a pop up or something else – demanding money or cryptocurrency to unlock files or threatening to release sensitive information to the public if you don't pay.	1. Never pay a ransom or communicate with the cyber criminal – there is no guarantee you will get access to your files or that they won't leak sensitive information. 2. Take a photo of your device screen or write down important details like the names and extensions of affected files, what the ransom note says, and anything else that has changed since the attack. 3. Turn off the infected device by holding down the power button or unplugging it and disconnect other devices from your network. 4. Contact an IT or cyber security expert to help you recover your information and remove ransomware from your devices. 5. Report the incident if required and notify anyone affected. Check signs of a data breach and follow steps to recover.

Common cyber threats

Threat/incident	What does it look like? (Symptoms)	What to do
Data breach: Private information is accessed and shared without permission.	• You receive a ransomware note threatening to release sensitive information • Your confidential data is found online • Unusual account activity • You can't log in to your accounts • Lots of files have been renamed, moved or deleted	1. Stop further information from being leaked, by containing the breach and securing your accounts and devices. If it looks like the breach happened because of malware or ransomware, follow steps to control it, or contact an IT or cyber security expert for help. 2. Quickly assess the types of information involved, how much information was shared and where, who will be affected by the leak and how it might cause harm. 3. Contact your local CERT, police or a legal professional for advice on what to do next and how you can tell people whose information has been stolen.
Account compromise: Someone gets unauthorised access to your email, banking or other accounts.	• Your passwords aren't working, you can't log in to your accounts, or you get logged out of your accounts • Changes have been made to your account that you didn't make • You receive an unexpected notification about a password reset or attempted login • Your bank account shows payments you didn't make or there is money missing • People say you sent them unusual messages.	1. Contact your bank to secure your money. 2. Check your account provider's website for advice to recover and secure your account. 3. If there are signs of malware, follow steps to remove it before changing passwords. 4. Log out of the compromised account on all devices, change your password and set up multi-factor authentication. 5. Secure any account that has the same password or is somehow connected to the compromised account, by checking for suspicious activity and changing your passwords. 6. Report any theft or other crimes to the police. 7. Report the incident to the account provider. 8. Keep an eye out for suspicious activity.
Business email compromise: Someone sends emails pretending to be from your organisation, by creating fake email accounts or by hacking into your email accounts	• Someone says they received an email from you or your organisation that you didn't send • Other signs of account compromise in your email account, like unusual login activity, unexpected password resets, or emails have been deleted or moved around.	1. Contact your bank to secure your money. 2. Follow account compromise steps to secure your account. 3. If you've been hacked or people are pretending to be you, let your contacts know so they don't fall for scam emails claiming to be from you. 4. Contact your local CERT, an IT expert or your email provider for help to get any fake accounts taken down.