Cyber breach reporting: What to do if you've been attacked

When a breach occurs, having a clear action plan can make all the difference when it comes to reporting the incident quickly and minimising the impact it has on your business and on any individuals affected.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

vodafone
business

This step-by-step checklist offers a practical, actionable timeline to guide your response, ensuring that you meet the necessary regulatory deadlines while protecting your business and your customers

Reporting a cybersecurity breach

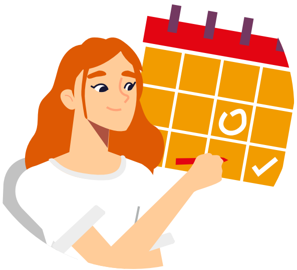
When a breach occurs, having a clear action plan can make all the difference when it comes to reporting the incident quickly and minimising the impact it has on your business and on any individuals affected.

This step-by-step checklist offers a practical, actionable timeline to guide your response, ensuring that you meet the necessary regulatory deadlines while protecting your business and your customers.

Within the first hour

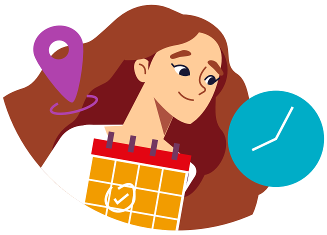
- Isolate affected systems to prevent spread.
- Notify your IT team or security provider.
- Begin documenting the incident with timestamps.
- Activate your incident response team.
- Preserve evidence and logs.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.



Within 24 hours

- Conduct initial impact assessment.
- Start detailed incident log with all actions taken.
- Determine scope of data or systems affected.
- Engage forensic experts if needed.
- Notify senior management and legal counsel.
- Identify which external stakeholders need to be informed (if any).



Within 72 hours

- Submit formal breach notification to your country's cyber reporting agency.
- Prepare communications for affected individuals (if required).
- Address vulnerabilities that caused the breach.
- Contact cyber insurance provider.
- Contact PR agency/communications team if needed.

Looking for more information?
Chat with our V-Hub advisers for 1-2-1 support and personalised advice.

Ongoing recovery

- Implement security improvements.
- Update policies and procedures.
- Conduct staff retraining.
- Monitor for ongoing threats.
- Review and test incident response plans.
- Implement full communications strategy.
- Manage media relations and public statements.
- Provide regular updates to stakeholders.

A fast, coordinated response is critical when facing a cybersecurity breach. This checklist is designed to help you act decisively under pressure—protecting your systems, complying with regulations, and maintaining trust with your customers and stakeholders.

For more information about reporting a cyber breach, get 1-2-1 support from our friendly V-Hub Digital Advisers.

Our V-Hub Digital Advisers are here to help.

vodafone
business