BreachReady
BY DFI FORENSICS

A GUIDE FOR BUSINESS AND FINANCE LEADERS

Email compromise

Protecting payments and confidential information



01 / MORE THAN A FRAUDULENT PAYMENT

Protect the information behind the transaction

A credible email can arrive from a familiar name, inside a genuine conversation, at exactly the moment a payment is due. The danger is not limited to a transfer. Unauthorized mailbox access can expose private correspondence, client records and attachments, and may open a route into connected cloud services.

BreachReady gives your organization retained DFI incident-response specialists before an incident, with priority support 24/7 from day one of an active annual agreement. Alongside that response relationship, DFI guides your team and IT provider on practical preparation and mitigation of business email compromise. The agreed scope governs the service. [1, 2]

THREE EXPOSURES TO CONSIDER

Money

Instructions may redirect a legitimate payment.

Information

Mailboxes can contain confidential records.

Trust

A genuine account can make fraud convincing.

Impersonation and account compromise are different

An attacker may use a lookalike domain or misleading display name without entering your systems. Alternatively, the attacker may control a real account or session. A suspicious email therefore does not, by itself, prove your mailbox was breached. Equally, a correct address and familiar wording do not prove the request is safe. The response needs to establish which situation exists. [3, 4]

The business process is part of the protection

Email security reduces exposure, but payment controls must remain effective when a believable message gets through. Finance should be able to pause a change without penalty, verify it independently and obtain approval that is separate from the request itself. Leadership needs to support that pause, including when the request appears to come from leadership.

If funds may already have moved

Contact your financial institution immediately through a trusted route and request its fraud response and recovery process. Do not wait for the technical investigation to finish. Recovery is not guaranteed. [4]

02 / PAYMENT VERIFICATION

Verify the change outside the email conversation

A reply to the same email thread can return to the attacker. So can a call to a new number included in the message or attached invoice. Payment changes need confirmation through a channel and contact detail established independently of the request. [4]

Use a trusted callback	Contact the known supplier or client using a previously verified number from a controlled record. Confirm the reason for the change and the relevant payment details. Do not replace the stored phone number on the strength of the same email.
Separate verification and release	Where feasible, use a second authorized person to approve the change and release the payment. Both people need to see the verification result, rather than merely approve the original email.
Control the supplier record	Limit who can amend payment details. Retain the request, the independent confirmation and the approval. Apply the same discipline to new suppliers, payroll changes, refunds and exceptional one-off payments.

Make exceptions harder to exploit

Set a documented escalation route when a known contact cannot be reached. A deadline or senior person's apparent request should trigger that route, not remove the control. If the organization chooses to proceed despite unresolved verification, an authorized decision-maker should explicitly own and document the risk. The safer default is to hold the affected payment.

A routine invoice with a new account

ILLUSTRATIVE SCENARIO / NOT A DFI CLIENT INCIDENT

An invoice has the expected amount and purchase reference, but the bank details have changed. The finance team calls the supplier through its existing vendor record. The supplier says no change was requested. Holding the payment and escalating the message protects the transaction without needing staff to prove how the email was created.

A familiar voice or video is not enough on its own. Use the agreed callback and approval process rather than relying only on recognition, urgency or the seniority of the person apparently asking.

03 / ACCOUNT AND INFORMATION SAFEGUARDS

Reduce opportunities for access and make suspicious activity visible

Ask your IT provider to explain how email and identity safeguards work in your actual environment. DFI can help prioritize the response and risk-reduction questions. The controls must have owners, appropriate configuration and a route for acting on alerts; a product licence alone is not evidence that protection is operating.

Stronger sign-in protection

Require multi-factor authentication for staff and administrators, using phishing-resistant methods where supported. Protect administrative access separately, remove unused accounts and restrict access to what each role needs. MFA reduces risk but does not make an account immune. [3]

Visibility into account changes

Configure appropriate alerts and review for unexpected sign-ins, forwarding and mailbox rules, privilege changes and connected applications. Decide who receives alerts and who can act when the usual administrator is absent. [3, 5]

Email and domain controls

Have your provider maintain filtering and supported email-authentication controls such as SPF, DKIM and DMARC. These can help address spoofing of your domain; they do not prove that every message is genuine or stop misuse of an already compromised account. [8]

Reduce what one compromised mailbox can expose

Move sensitive working records to approved systems with appropriate access controls instead of repeatedly circulating copies. Review delegated mailbox access and external sharing. Apply retention rules with business, legal and regulatory needs in mind; do not improvise deletion after a suspected incident.

Preserve the ability to investigate

Confirm which sign-in, mailbox, administrative and cloud activity records are available, how long they are retained and who can preserve them. Retention and event coverage depend on the service, licensing and configuration. If the evidence expires, the organization may lose the ability to narrow the incident or explain what information was affected. [5]

04 / WHEN COMPROMISE IS SUSPECTED

Stop further harm and investigate the account

Treat a credible report as a reason to activate your response arrangements, not as a reason to make public conclusions immediately. Finance, IT, retained specialists and the privacy or legal lead may all have work to do. Keep urgent protective action moving while preserving the records needed to understand the event. [4, 5]

Protect the transaction and the conversation

Hold affected pending payments and contact the bank immediately if money may have been sent. Reach the purported sender through a trusted route. If account access is suspect, use a separate verified communication channel for the response. Do not send reset credentials or sensitive incident details into a mailbox that may still be accessible to the attacker.

Have authorized responders regain control

The technical team should assess account restriction, session revocation and credential changes, together with the service's current remediation guidance. Investigate persistence through forwarding, mailbox rules, authentication methods, delegated access and connected applications. A password reset alone may not remove every route back in. Coordinate collection of relevant logs and settings with urgent containment. [5]

A COORDINATED RESPONSE

Finance

Contain payment risk and speak to the bank.

IT and specialists

Restrict access, preserve and investigate.

Leadership and counsel

Assess impact, duties and communications.

Keep the original records

Preserve suspicious messages with their headers, attachments and relevant transaction records. Capture the time noticed and actions already taken. Do not rely on a screenshot or forwarded message as the only record. Use an approved secure transfer route for evidence, and limit access to the people who need it.

Report without waiting for complete certainty

Use the appropriate police and fraud-reporting routes in consultation with your response team. In Canada, attempted or completed fraud can be reported to local police and the Canadian Anti-Fraud Centre. [6]

05 / EXPOSURE AND RETURN TO SERVICE

A restored mailbox does not close the incident

Once access is controlled, the organization still needs to establish the likely period and scope of compromise. What could the account access? Which activities are supported by logs? Were messages sent, rules changed or files reached? Examine connected services where relevant; the mailbox may not be the whole incident. [5]

Distinguish access from proven disclosure

Account compromise may create an information exposure even if no fraudulent payment occurred. Available records can support a conclusion about access, sending or other activity, but may not show every message read or item copied. Missing logs do not prove that nothing happened. Describe the evidence and its limitations when assessing harm or making statements to clients.

Make privacy assessment an explicit workstream

Identify the categories of personal and confidential information involved, the people affected and plausible consequences. Counsel and the privacy lead should assess applicable law and contracts. Where PIPEDA applies, breaches creating a real risk of significant harm require reporting and notification, and records of all breaches must be kept. Do not assume that stopping the payment resolves those obligations. [7]

No money lost, but client information at risk

ILLUSTRATIVE SCENARIO / NOT A DFI CLIENT INCIDENT

A fraudulent request is caught before payment. The investigation nevertheless finds unauthorized access to a mailbox holding client correspondence. The useful next decision is not whether to celebrate a blocked fraud. It is how to assess the information at risk, protect affected people and determine any required notices.

Restore trust in the process

Before normal use resumes, the technical lead should confirm the planned containment and remediation work, remaining risks and follow-up monitoring. Leadership should confirm that finance and client-facing staff know the updated instructions. Rehearse the failed hand-off, review payment controls and track corrective work to completion. Keep uncertainty visible until the evidence supports closing it.

06 / SPECIALIST HELP AND REFERENCES

Make email protection a business capability

BreachReady combines retained specialist response support with preparation that addresses business email compromise, ransomware and the decisions around them. DFI works alongside your existing IT provider and leadership to build a coordinated plan and rehearse it. Practical safeguards and payment verification help reduce exposure before a crisis; no program eliminates every risk. [1, 2]

Bring your current payment-approval process, email platform, IT support arrangements and confidentiality concerns. We can discuss the most useful preparation for your organization and where specialist support would fit.

Talk through your current arrangements

dfiforensics.ca/contact | 778-742-5621 | info@dfiforensics.ca

If an incident is underway, existing BreachReady clients should use their agreed response arrangements. Others can visit dfiforensics.ca/incident-help. An inquiry does not create an engagement or guarantee a response time. Do not send passwords or confidential evidence with an initial inquiry.

Sources and further reading

Primary sources checked 9 November 2026. General preparation guidance, not legal advice or an assessment of your organization. Apply current service documentation, law and agreed engagement terms. Sources do not imply endorsement of DFI.

[1] DFI Forensics | BreachReady
Annual preparedness and response program; specialist and IT-provider roles.

[2] DFI Forensics | What BreachReady includes
Response planning, playbooks, exercises and continuing readiness support.

[3] Canadian Centre for Cyber Security | Managing email
Email threats, account protection and compromise response, ITSAP.60.002.

[4] FBI | Business email compromise
Independent payment verification and prompt bank contact.

[5] Microsoft | Respond to a compromised cloud email account
Account containment, persistence checks and investigation.

[6] Canadian Anti-Fraud Centre | Spear phishing
Impersonation and payment-redirection fraud.

[7] Office of the Privacy Commissioner of Canada | Breach reporting
PIPEDA reporting, notification and record-keeping obligations.

[8] FBI IC3 | Cloud-based email compromise
Email-domain authentication and independent payment verification.