A practical business guide for Irish SMEs

Social Engineering and Phishing

Protect your payments, accounts and information by making verification part of everyday work.

Recognise **Verify** **Report**

Written for Irish SME owners and managers, with sections for employees and for your IT provider. Irish evidence, European context and international threat research.

Start with the decisions that matter

Social engineering turns ordinary work into an opening for fraud. It succeeds because each request resembles something you already do. These are four moments to recognise.

A supplier asks to change its bank details.

The invoice can be genuine while the account belongs to a criminal.

A manager asks for a confidential favour.

Secrecy removes the colleagues who would normally check.

Someone claiming to be IT support asks for a code.

A code or an approval can hand over your account.

A senior leader wants an urgent payment or sensitive file.

Authority and urgency are used to skip the usual check.

One response to all four: agree these three rules today

1 Recognise

Treat any request to move money, change payment details, share codes or confidential information, install software, grant access or skip a procedure as consequential.

2 Verify

Check bank-detail, sign-in and remote-access requests through a contact route that existed **before** the request arrived. Never approve an unexpected prompt.

3 Report

Report suspected mistakes and near misses immediately, even if you are unsure whether anything happened.

The full framework is on page 3.

Find your part of this guide

FOR EVERYONE	**Pages 3, 7–9, 11–17.** The framework, what pressure looks like, practice exercises and your checklist.
FOR MANAGEMENT	**Pages 3–6, 10, 18, 20–24.** The business risk, payment controls, culture, response and your 30-day tracker.
FOR YOUR IT PROVIDER	**Pages 12, 19 and 21.** The identity and Microsoft 365 controls to review, and the evidence to ask for.

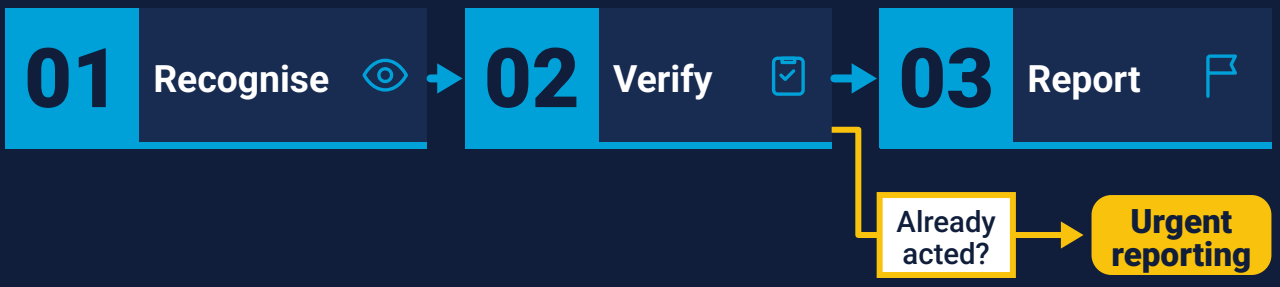
Incident happening now? Go straight to page 21. **Short on time?** Read pages 2–3, then run an exercise from pages 14–16 with your team.

This guide is general information, not legal, regulatory or professional advice, and it cannot guarantee any outcome. Adapt it to your organisation and take advice on your circumstances. The exercises are fictional training scenarios, not reported IT.ie customer incidents.
Evidence reviewed to 30 October 2026 · Version 1.0 · November 2026.

FOR EVERYONE FOR MANAGEMENT

Recognise. Verify. Report.

Use this whenever a message, call or visit asks you to move money, share information, sign in, approve access or bypass a normal process.



1 Recognise a consequential request

Ask what happens if you comply. Could money move, a password or code be disclosed, confidential information shared, software installed, access granted or a normal procedure bypassed?

Urgency, secrecy and "don't contact the usual person" are signals. You do not need a full diagnosis: an unexpected request with a material consequence justifies a pause, even if it contains no obvious error.

2 Verify through a route you choose

Use contact details you already hold: a supplier record, staff directory, saved bookmark or approved app. **Never use the number, address or link supplied in the request.**

Confirm both the identity and the authority for the specific action. If you cannot confirm it, hold it and escalate.

3 Report quickly through a known route

Report suspicious activity, mistakes and near misses straight away. If you entered credentials, approved a prompt, sent money, shared data or installed anything, use the urgent route, not a routine ticket.

Say what happened, when, and which account or device. Keep the original message and do not forward it. Early reports help the business contain and recover.

Make reporting easy to start

Suggested employee wording

"I may have acted on a suspicious request at [time]. I used [account or device] and [describe the action]. Please help me contain it. I still have the original message."

Employer setup · for management

Publish one routine reporting route, one urgent telephone route and an out-of-hours alternative, and test all three. Say clearly that reporting a good-faith concern is welcome, even when it proves harmless. Staff can only verify if you give them time, a trusted contact record and support for the pause.

FOR MANAGEMENT

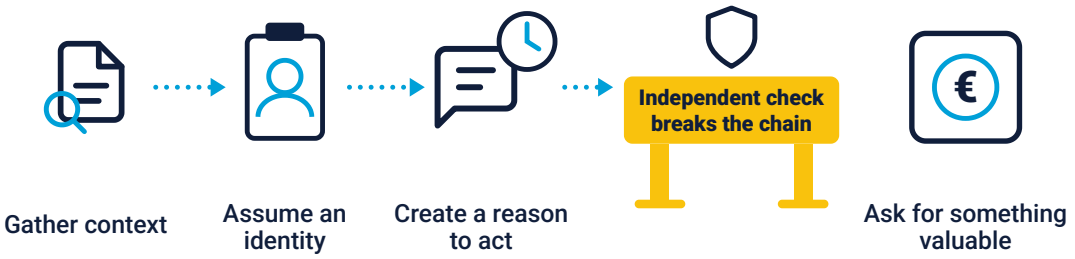
Understand the business risk

Social engineering is deception that influences someone to take an action that benefits an attacker: sending money, sharing information, handing over an account or opening a door. **Phishing** is one method: a deceptive message prompts the recipient to act.

Phishing does not need malware. A short email asking accounts to amend a supplier record can divert a legitimate payment. Attackers also use real accounts they have taken over, so a familiar sender or an existing email thread is not proof that a new instruction is genuine.

How a request becomes an incident

An attacker gathers context, assumes an identity, creates a reason to act and asks for something valuable. It can take minutes or several conversations, and broad untargeted messages work too.



Consider the sequence: a supplier's name appears on a project announcement; an email refers to that project; a call says an invoice is overdue; new bank details arrive. Each step looks professional. The danger is accepting the change without independent confirmation.

What can be lost

- Money can move to a criminal's account through an apparently authorised payment.
- A stolen account can expose email, customer records and documents, and be used to target others.
- Malicious software can disrupt operations or steal information.
- Recovery consumes management time and can interrupt payroll, deliveries and customer service.

Put responsibility in the right place

Staff make these decisions inside the systems and pressures management creates. Training helps, but they also need time to verify, a trusted contact directory and a manager who supports a pause. Filtering, strong authentication, payment approvals and a tested response plan should back those decisions up.

✓ Take action

Identify the three requests in your business that could cause the greatest harm if accepted without checking. Agree a verification rule for each.

Source foundation: the two earlier IT.ie guides [1, 2].

FOR MANAGEMENT

Ireland and Europe in context

Ireland

€179.04m

fraudulent payments in 2025, from €140.80m in 2024

Central Bank of Ireland

Irish payment fraud is a business warning

The Central Bank of Ireland reports that payment fraud rose 27.2% in 2025. The figure covers all fraud types reported by Irish-resident payment providers, not business fraud alone. [4]

For an SME, the lesson is operational: a real employee can authorise a fraudulent payment because they were manipulated. Protect the decision to pay, not just the banking login.

European Union

ENISA
Threat Landscape 2026

CERT-EU
Threat Landscape Report 2025

European reporting shows several routes into a business

ENISA reports continuing phishing, commercially available phishing kits, ClickFix fake-verification tricks and risks that travel through suppliers and connected services. [5]

CERT-EU shows social engineering reaching beyond email: voice phishing, AI impersonation, malicious application permissions and ClickFix. Its findings come from EU institutions and their partners. [6]

International

Microsoft
EvilTokens campaign research

International evidence makes identity a priority

Microsoft's September 2026 investigation of EvilTokens documents device-code phishing, and AI used to tailor messages and examine compromised inboxes. Attackers can abuse a genuine sign-in process, not only a fake login page. [7]

Our recommendation

Treat payment instructions, account recovery, new application access and remote-support requests as verification points across every channel. Ask your IT provider how those decisions are protected and monitored.

Each source covers a different period and scope, so the figures are shown separately. Dates and scope are in the references. Sources: [4, 5, 6, 7].

FOR MANAGEMENT

What Irish office workers told us

CyberPulse Ireland 2025 is IT.ie's research with SonicWall. Censuswide asked 1,000 office workers in Ireland how security works in practice. Here is what they said, and what to do about it. [3]

20% — Workers who caused a breach

Of the workers who said they had caused a data breach, 20% said they had fallen victim to a phishing email in the previous 12 months.

→ **Practise real requests, such as a bank-detail change.**

36% — All respondents

Office workers said they had not reported a breach in the previous 12 months. The top reason was embarrassment, then fear of repercussions.

→ **Make reporting quick, easy and safe.**

20% — All respondents

Office workers said they had not received cybersecurity training for more than a year, or ever.

→ **Check everyone is covered, including new starters and temps.**

73% — All respondents

Office workers believed their employer holds staff personally responsible for incidents, always or sometimes.

→ **Tell staff plainly: report honestly and you will get help.**

58% — All respondents

Office-based employees felt more vulnerable to cyberattacks when working remotely.

→ **Make the helpdesk as easy to reach from home as from the office.**

65% — All respondents

Office workers said they used work devices for personal tasks in the previous 12 months.

→ **Set simple rules for devices and accounts.**

What to do with this

Make it safe to speak up. Say plainly that good-faith reports get help and fair treatment. Give everyone one routine and one urgent route, and test both this month.

Make verification part of normal work. Agree a callback rule for bank-detail changes and unexpected sign-in prompts, then practise it with the exercises on pages 14–16.

Self-reported survey of 1,000 office workers in Ireland. The 20% phishing figure is a share of workers who said they had caused a breach, not of all workers. Sources: [3]. Full report: it.ie/cyberpulse-ireland-2025.

FOR EVERYONE

Why convincing requests succeed

Social engineering exploits ordinary working habits: helping a colleague, answering a customer, respecting a manager and meeting a deadline. An attacker makes the requested action feel more important than the normal check.

Recognise the pressure being applied

Authority	A caller claims to be the managing director, a solicitor, a bank or your IT provider. Their role is used to discourage questions.
Urgency	A payment must leave before a cut-off, or an account will close. The aim is to shrink the time available for verification.
Secrecy	An acquisition, disciplinary matter or payment "must stay confidential". Privacy can be legitimate, but it should not remove required controls.
Familiarity	A colleague's name, a genuine invoice or real project details make the story believable. Only an independent check confirms authority to change a payment or share data.
Helpfulness	Someone needs you to solve a problem, accept a parcel, install a support tool or let them through a door. A small first request can lead to a bigger one.

Judge the request, not the look

Grammar, logos, caller ID, a familiar voice and even polished AI-written text can all be copied. The padlock (HTTPS) shows a connection is private, not that a website is honest, and an external-email banner is a prompt to take care. **Ask what you are being asked to do, then verify that action through a separate route.**

Make a pause socially acceptable

FOR MANAGEMENT

> **"I can help once I have completed our verification check."**
>
> This gives employees language they can use with a real senior manager as well as an impersonator. Leaders should show that the rule applies to them.

If the normal approver is absent, use a documented deputy. If the trusted contact cannot be reached, hold the action and escalate. If someone refuses a check, treat that as a warning. You never need to prove fraud before pausing.

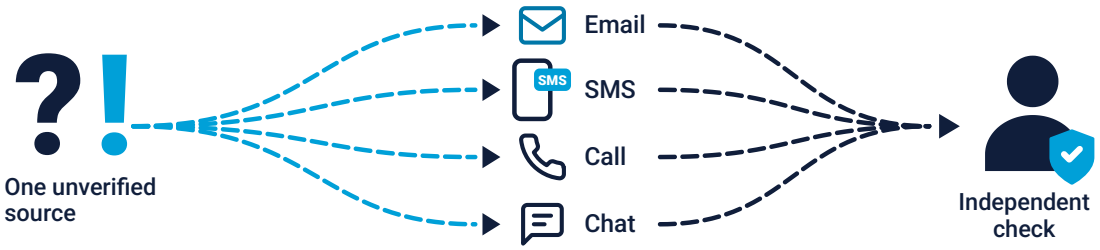
Team exercise: Ask whether a junior employee could comfortably delay a director's payment request. If the answer is no, change the process before testing the employee.

Source foundation: [1, 2].

FOR EVERYONE

An attack can change channels

The same deception may move between email, phone, text and collaboration tools. **A second message from the same unverified source is not independent confirmation.**



Channel or technique	A plausible request	A safer response
Email and targeted phishing	Review a contract, resolve an invoice or reset a password.	Open the known business service yourself and verify unexpected requests.
SMS and messaging apps	Pay a delivery charge or contact a manager on a new number.	Use your existing contact record or official app.
Voice phishing	Your bank account is at risk, or IT needs a code.	End the call and initiate contact through a trusted route.
Teams and other collaboration tools	An external support agent offers to fix a fault.	Contact your own helpdesk before sharing a screen or granting control.
QR codes	Scan to access a document, pay a charge or renew MFA.	Check the context and destination; prefer the known app or website.
Physical impersonation	A visitor needs entry, a badge or access to equipment.	Follow visitor procedures and contact the named host.

A few useful terms

Spear phishing is tailored to a person or group. **Whaling** targets senior or high-value roles. **Pretexting** creates a false story, such as an audit or support case. **Baiting** offers something attractive, such as a free download or a USB device. The label matters less than the action requested.

Keep remote working within the same rules

Use approved devices and access methods, and keep work information out of personal accounts unless authorised. Save support numbers somewhere you can reach if email is down. Never move a work task to a personal phone because a message tells you to.

An attack can also begin with a search advert or a compromised website, so a link is not trustworthy just because a search engine returned it. **Use saved bookmarks for banking, payroll and frequently used business systems.**

Source foundation: [1, 2]; evolving channel context [6].

FOR EVERYONE

Read the request as well as the message

Inspecting an email can reveal warning signs, but the key question is **what the sender wants you to do**. A genuine account may be compromised, and a legitimate file-sharing service can deliver a malicious link.

A realistic phishing example

Subject **Invoice HP1048 - Updated Payment Details** 1 October 14, 2026 10:18 AM

From **Harbour Projects** <accounts@harbour-projects.example> 4

To **Team** <team@company.example>

Hi team,

please find attached invoice HP1048 for recent project milestones. Please note our bank details have been updated due to our **year-end audit**. Kindly process payment by 5pm today as I will be unavailable by phone this afternoon. 2 3

Regards,
Harbour Projects

Invoice_HP1048.pdf (142 KB) 5

Illustrative message, fictional names and a reserved example domain. A compromised real sender can look completely normal.

What deserves attention

1. The request changes where money will go. That triggers verification even if the email address is correct.
2. The audit story gives a reason to depart from established records.
3. The deadline and claimed lack of phone access discourage an independent check.
4. A reply would return to the same potentially compromised channel.
5. An attachment, signature or genuine invoice number does not validate the bank account.

Sign-in requests

Open the service through a trusted bookmark or app. Hovering over a link on a computer may reveal its destination, but on a phone inspection is awkward, and you should not open a suspect destination just to investigate it. **URL inspection is an aid, not a substitute for a trusted route.**

What to do next

Hold the change. Call the supplier on a number already recorded in your supplier master file. Confirm with the appropriate authorised person, record the check and use the normal approval process. If the change cannot be confirmed, escalate to finance and report the message to IT.

Source foundation: [2]; payment controls [8].

FOR MANAGEMENT FINANCE LEAD

Protect supplier payments and payroll

Business email compromise (BEC) uses business identities and conversations to obtain money or information, through a compromised mailbox, a spoofed address or an impersonator. Common targets are supplier payments, payroll bank details and supposedly confidential executive transactions. [8]

A payment change needs its own approval

Check the invoice and the destination account separately. A genuine invoice can carry fraudulent bank details, and matching it to an order does not verify a new payee.



Adopt a written rule

Every bank-detail change is held until independently verified. Use an existing supplier record or a previously established secure portal, never the number, link or contact details supplied with the change. Record who checked, whom they contacted, when and what was confirmed.

Design a process a small team can follow

The person who requests or enters a bank change should not be its only approver. In a very small business, use the owner or a nominated deputy for the independent check. Set payment approval thresholds, review unusual or first payments, and do not let a senior title waive the controls.

Control access to supplier records and review recent changes before each payment run. Apply the same checks to payroll changes, refunds and requests to pay a third party. A bank's payee-name check is useful, but a match does not prove the request is legitimate.

If a payment has already left

Contact the bank's fraud team **immediately** through an established route and request an urgent stop or recall. Give the amount, time, beneficiary details and transaction reference. Alert finance leadership and IT, preserve the communications and report suspected crime to An Garda Síochána. Recovery is not guaranteed. [8]

Recommended finance test

Take one recent supplier change and trace the independent verification and approval evidence. If the trail ends with "confirmed by email", improve the process.

Sources: [8]; the payment and impersonation foundations in [1, 2].

FOR EVERYONE

AI makes identity harder to judge

Generative AI can write fluent messages, imitate a writing style and produce synthetic voices or video, often combined with public information or stolen correspondence. CERT-EU places AI impersonation within an evolving social-engineering landscape; Microsoft documents AI-assisted phishing and analysis of compromised mailboxes. [6, 7]

That does not mean every polished email is AI-generated or every odd call a deepfake. The rule is unchanged: **verify the requested action**, without relying on your ability to tell how the content was made.

Three situations to prepare for

A persuasive message

An email cites a real project in a director's usual phrasing. Verify anything that changes payment, access or disclosure through your established workflow.

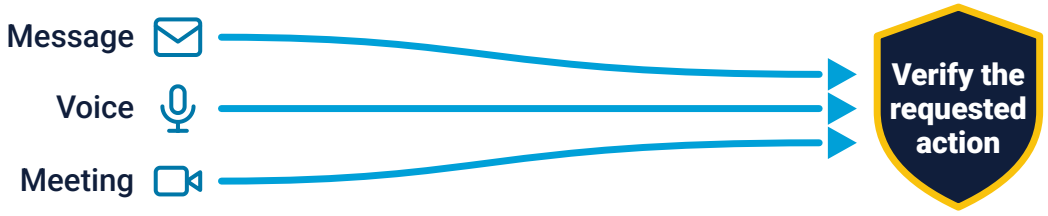
A familiar voice

A caller sounds like someone you know but asks for a transfer or a confidential file. End the call and use a trusted directory entry. Voice and caller ID are not proof.

A convincing meeting

Apparent colleagues ask you to bypass an approval. A meeting is not verification: confirm through independently initiated contact and follow the normal process.

Message, Voice, Meeting: One Procedure



Do not build your defence around visual clues

Odd lip movements or unnatural phrasing may raise suspicion, but their absence proves nothing, and poor video is common in legitimate work. An agreed verification phrase adds a check, but it can be overheard or disclosed. It cannot replace independent contact and payment approval.

Reduce useful exposure

Be thoughtful about publishing staff responsibilities, travel plans, internal screenshots and project details.

Do not upload confidential correspondence to an unapproved AI service to ask whether it is a scam. Use your organisation's reporting route so the message can be examined safely.

Sources: [6, 7].

FOR EVERYONE

Microsoft 365 attacks target trust

A business account can give an attacker access to conversations, files and other people's confidence. Protection has to cover **sign-ins, permissions and what happens after access is obtained.**

Fake sign-ins and session theft

A phishing page may imitate a Microsoft sign-in. In what is technically called an adversary-in-the-middle attack, the criminal passes your real sign-in through their own site and copies the proof that you are signed in (a "session token"), so they can get in without your password or MFA code again. [5, 12]

Open services through known routes. If a document unexpectedly asks you to sign in again, stop and verify. Ordinary MFA is valuable, but not every method resists phishing.

Unexpected approvals and codes

Repeated prompts can pressure someone into approving an attacker's sign-in. Reject unexpected requests and report them. Never read out a code or enter a number because a caller tells you to. [9, 12]

Permissions can expose data too

A consent screen may ask to read mail or access files. It can be genuine Microsoft infrastructure while the application, or the reason for granting access, is untrustworthy. Do not approve an unfamiliar app just to view an invoice; ask IT to assess it. [11]

A genuine login page can still deceive

Device-code phishing asks you to type an attacker-supplied code into a real Microsoft sign-in page. That approves the attacker's access, not yours. Use device-code sign-in only for a device or application you are deliberately setting up through an approved process. [7]

If you already acted

Tell IT exactly what you entered, approved or installed and when. A password reset alone may not remove malicious permissions or end every form of access. **Response actions are on page 21.**

For your IT provider

The controls that reduce these risks are on page 19. **You do not need to configure them. You do need to know whether someone has.**

Sources: [5, 7, 9, 11, 12, 13].

FOR EVERYONE

New packaging for familiar deception

QR code phishing

A QR code hides its destination until it is scanned, and scanning moves the task to a phone, outside normal work protections. Open the relevant service yourself instead. If scanning is part of an approved workflow, check the destination and purpose. **A QR code is a link format, not evidence of trust.** [2]

ClickFix and fake verification

ClickFix presents a supposed fault, browser update or human-verification check, then persuades the user to run commands or install software. ENISA identifies it as an observed technique. [5]

No website needs you to paste commands into a system window to prove you are human. Close the page and report it. If you ran a command or installed something, stop using the device and contact IT immediately; do not try to undo it yourself.

Fake support and remote access

A caller may claim to be fixing spam or responding to an alert, sometimes after a problem was deliberately created. Legitimate remote-support tools can be abused as easily as malicious ones.

Verify the support case through your known helpdesk before installing anything, sharing a screen or granting control. Never let an unverified caller watch a banking session or see authentication codes. Tell IT if access was granted, even briefly.

Trusted platforms and shared documents

A file on a recognised service can still contain a malicious link. Treat unexpected sharing invitations, calendar requests and requests to move a conversation to another app as you would email: did you expect it, and do the requested permissions make sense?

For management

Publish the support tools your organisation uses and the process for starting a session. Give staff a reliable alternative when a caller claims the usual helpdesk is unavailable.

Sources: [2, 5, 6]. The support workflow is a recommended organisational procedure.

1

IT.IE DECISION EXERCISE 1

The supplier bank change

Run this with your team. Illustrative training scenario: names and events are fictional.

Situation

A small engineering business is preparing its Friday payment run. A long-standing supplier emails updated bank details, quoting the correct invoice number and project, in an existing email thread. A follow-up caller says the old account has been closed and asks accounts to act before lunchtime.

Decision point

Do we change the supplier's bank details because the invoice, the thread and the caller all look right?

A genuine invoice or familiar conversation does not verify a new account. The mailbox could be compromised, and the caller may be part of the same attempt.

Recommended response

The employee holds the change and calls the supplier on the number already recorded in the supplier file. The established contact denies making the request. Accounts informs the finance lead and IT, preserving the email and the time and number of the follow-up call.

A second approver signs off any verified details before payment is released, and the original payment stays on hold until finance confirms a safe destination. IT checks whether other staff received the request and whether the business's own account may be involved. The supplier is contacted through a trusted route so it can investigate its side.



If the transfer had already been made

Call the bank's fraud team first to seek an urgent stop or recall; do not wait for a full internal investigation. In parallel, organise technical investigation, preserve evidence and report the suspected crime. See page 21.

Questions for the team

- [ ] Where is our trusted supplier contact record, and who can change it?
- [ ] Who approves a new account when the finance manager is absent?
- [ ] Would our process catch a genuine invoice with substituted bank details?

Success measure: The employee pauses because the payment destination changed, not because they spotted a spelling mistake.

Scenario informed by the payment-fraud concepts in [2, 8].

2

IT.IE DECISION EXERCISE 2

The helpful support agent

Run this with your team. Illustrative training scenario: names and events are fictional.

Situation

A professional-services employee receives a burst of unwanted emails. Soon afterwards, a Teams message arrives from someone claiming to be the company's support partner. They offer to remove the spam and ask the employee to start a remote-support session.

The caller is knowledgeable and knows the employee's name. During the session they ask the employee to enter a code into a sign-in page and approve a prompt so that "the security repair can finish".

Decision point

Do we start a remote session because the caller knows our name and the tool and sign-in page are real?

None of that authenticates the request. The employee raised no support case and has not confirmed the caller through the helpdesk.

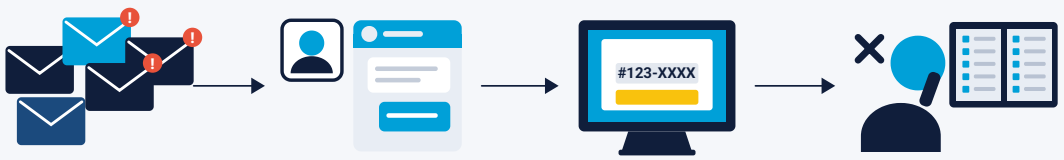
Recommended response

The employee ends the conversation without starting remote access. They use the helpdesk number saved in the company directory to check whether a case exists and whether that technician is assigned. The helpdesk confirms that no such work was requested and investigates.

The employee preserves the sender details and times, and does not keep chatting to gather information. The company warns other staff through its own trusted channel.

If access was already granted

Tell IT immediately that remote control was allowed, and describe any codes, prompts, downloads or permissions involved. Stop the session and, if safe, disconnect the device from networks, then call from another device. Do not wipe or restart it unless the response team directs you.



Spam burst | Support partner message | Remote session code | Call company directory

Questions for the team

- [ ] Can every employee identify the approved helpdesk route?
- [ ] What should a technician do to establish that a session is authorised?
- [ ] Can IT investigate a report if the employee cannot access email?

Success measure: The employee validates the support case before allowing control, rather than trusting a platform logo or a convincing explanation.

Scenario informed by [6, 7]; response considerations [13].

3

IT.IE DECISION EXERCISE 3

The director on a call

Run this with your team. Illustrative training scenario: names and events are fictional.

Situation

An accounts employee receives a call that sounds like the managing director. The caller mentions a real business trip and asks for an urgent payment for a confidential acquisition. A message with beneficiary details follows. The caller says the finance manager already knows and should not be disturbed.

The voice could be synthetic, an impersonation or someone exploiting a poor connection. The employee does not need to work out which before applying the payment rule.

Decision point

Do we release the payment because the voice sounds like the managing director?

The request combines **authority, secrecy and urgency**, asks for an exception to normal approval and discourages contact with another approver. Those features matter more than how convincing the voice is.

Recommended response

The employee explains that all exceptional payments need the standard check, ends the call and contacts the director on a previously established number. They also consult the nominated finance approver through the usual workflow. No payment is released while confirmation is outstanding.

The real director confirms that no payment was requested. The employee reports the call and preserves the message, caller details and timing. Management backs the decision to pause and reviews whether travel information or public project details made the approach credible.

If the request is genuine

The same checks still apply. A real director can complete them or appoint an authorised deputy. If senior staff routinely bypass controls, employees cannot tell a legitimate exception from an attacker's story.

Two paths, one gate



Questions for the team

- [ ] Do staff have explicit permission to challenge a senior request, and do directors follow the same payment rules?
- [ ] Who can authorise an urgent payment during travel or leave?
- [ ] What happens when the person who appears to be calling refuses a callback?

Success measure: The employee protects the decision process without needing to prove that the voice is fake.

Scenario informed by [1, 6, 8].

FOR EVERYONE

Everyday checklist for employees

Use this checklist when joining the business and revisit it after a role or device change. If an item cannot be completed, ask your manager or helpdesk for support.

Recognise and verify: before you act on a request

- [ ] I verify changes to bank details, payroll and sensitive data-sharing instructions through an established route.
- [ ] I pause when a request asks me to bypass approval, keep unusual secrecy or move to an unfamiliar channel.
- [ ] I open banking, payroll and work services through known apps or saved bookmarks.
- [ ] I confirm unexpected support requests before sharing my screen, installing software or allowing remote control.

Report: when something goes wrong

- [ ] I know how to contact the helpdesk without relying on the affected email account.
- [ ] I report immediately if I click, enter information, approve access, send money or disclose data in a suspicious interaction.
- [ ] I describe what happened accurately and preserve the message. I do not try to investigate the attacker or hide a mistake.

When using accounts and devices

- [ ] I use unique passwords stored in an approved password manager, or approved passkeys where available.
- [ ] I use MFA and reject unexpected prompts. I do not share codes or approve a sign-in for someone else.
- [ ] I refer unfamiliar application permissions and device-code requests to IT.
- [ ] I use approved devices and install updates through the organisation's normal process.
- [ ] I follow the company rules for personal use, removable devices and working away from the office.
- [ ] I lock my device when leaving it and follow visitor procedures rather than letting an unverified person follow me into a restricted area.

Keep a small contact record

Routine reporting route _____

Urgent helpdesk number _____

Out-of-hours contact _____

Manager or deputy _____

Store a copy where it remains accessible during an email outage. Your employer should supply and maintain these details; do not take them from an unsolicited support message.

Checklist adapted from the principles in [1, 2, 14] and the identity guidance in [9, 11, 12].

FOR MANAGEMENT

Management checklist with clear ownership

Record an owner and due date for every gap. Buying a service does not establish who will investigate an alert or make an urgent decision.

You do not need to configure these controls. You do need to know whether someone has: whether it is implemented, whether it covers all relevant users, who owns it, how it is tested and what evidence shows it works.

Control to confirm	Accountable role	Evidence to request
Independent verification of bank and payroll changes	Finance lead	A recent change with callback and approval records
MFA and access removal for leavers	IT owner	Account coverage, exceptions and a recent leaver check
Email domain protection and filtering	IT provider	Review of SPF, DKIM and DMARC, plus unresolved issues
Device updates and protection	IT owner	Coverage report and action on unsupported devices
Backups and recovery	Operations lead	A successful restore test for a critical system
Reporting and escalation	Business owner	A tested urgent route, including out-of-hours coverage
Training and verification procedures	Managers	Attendance, staff feedback and scenario outcomes
Incident and regulatory decisions	Incident lead	Named deputies, contact list and reporting criteria

Make the controls work together

Ask whether the person who can change a supplier account can also approve its first payment. Check that delegated and supplier access is necessary and reviewed.

SPF, DKIM and DMARC make it harder to send email pretending to come from your domain. They do not stop compromised accounts or lookalike domains, so pair them with independent verification.

Recommended review rhythm

Review urgent gaps weekly for the first month (tracker, page 23), then set a recurring review.

Backups support recovery, but do not prevent data theft or reverse a fraudulent transfer. Agree what must be recoverable and how much recent work the business can lose.

Measure outcomes, not activity

Track overdue bank-change reviews, uncovered accounts, unresolved critical alerts and restore-test results. A dashboard is not evidence that the work has happened.

Sources and foundations: [1, 2, 8, 14].

FOR YOUR IT PROVIDER

Strengthen identities and Microsoft 365

Hand this page to your IT administrator or provider as a review brief. Ask for a proposed rollout, any licence requirements and a way to show that each control works.

For management: you do not need to configure this. You do need to know whether someone has. Ask your provider, for each control: is it implemented, does it cover all relevant users, who owns it, how is it tested and what evidence shows it works?

Weaker	Weaker	Reduces accidents	Phishing-resistant
SMS codes	**Standard push**	**Number matching**	**Passkeys · WHfB · CBA**

Move towards phishing-resistant authentication

Microsoft Entra supports phishing-resistant methods including FIDO2 passkeys or security keys, Windows Hello for Business and suitable multifactor certificate-based authentication. Passkeys bind authentication to the intended service, helping prevent credential phishing; SMS codes and standard push approvals do not offer the same protection. [9, 10, 12]

Start with administrators, finance and senior decision-makers, then broaden coverage. Plan secure enrolment and recovery so a caller cannot obtain a reset by persuading the helpdesk. Keep protected emergency-access accounts, monitor their use and test recovery before enforcing new policies. Pair this with the payment controls on page 10.

Enforce the intended sign-in method

Where licensed, Conditional Access can require a phishing-resistant authentication strength. At the time of writing (October 2026), Microsoft documents an Entra ID P1 requirement for Conditional Access; check its current documentation and confirm what your subscription supports. Pilot policies and avoid locking out legitimate users. [9]

Close alternative routes to access

Review whether device-code authentication is needed. Microsoft recommends blocking it as broadly as practical, with documented, secured exceptions, and testing before enforcement. [15]

Restrict application consent according to business need and permission risk, with an administrator approval route. A verified publisher is useful context, not a guarantee. Review existing grants as well as new requests. [11]

Monitor what happens after sign-in

Assign responsibility for suspicious sign-ins, new authentication methods, unexpected devices, mailbox forwarding, inbox rules and application grants. Keep logs long enough to support investigation, within your licensing and data-protection arrangements. Remove obsolete accounts and unnecessary privileges.

Ask for a demonstration

Can your provider identify and contain a suspected mailbox compromise, including malicious permissions and persistent access, rather than only reset the password? [13]

FOR MANAGEMENT

Build a culture that encourages reporting

CyberPulse respondents described gaps in training and reluctance to report. Ask how easy it is to raise a concern in your own workplace, and what you would change. [3]

Start with a management commitment

Make this promise explicit: staff who promptly report a good-faith mistake will receive help and fair treatment.

Explain how this differs from deliberate misuse. Thank people for useful reports, and avoid public naming, humiliating exercises or league tables of individuals.

When someone reports a concern, acknowledge it, say what they should do next and close the loop when practical. A reporting button that leads to silence will not build confidence. Include agency workers, contractors and people who work outside office hours.

Teach decisions that match each role

Finance should practise a bank-detail change, HR a payroll amendment and an information request, and managers an urgent request that still needs approval. IT support should rehearse identity verification during a reset. New starters need these procedures before they receive sensitive access.

Use short refreshers after relevant changes or incidents, alongside periodic training. Choose a rhythm you will keep, and check understanding through realistic conversations.

Use simulations to improve the system

Set a clear purpose, protect employee privacy and give a constructive debrief. Avoid exploiting personal distress or collecting real passwords. Examine whether staff could find the reporting route, whether reports were answered and whether an approval process held up under pressure.

Click rates alone can mislead: someone who reports immediately after clicking may help contain an incident. Measure reporting and response alongside recognition.

Team discussion

"What would make it difficult to stop and verify a request here?" Invite specific examples of workload, hierarchy, missing contact details and inaccessible support. Assign an owner to remove each obstacle.

Source foundation: [1, 2, 3]. Training and review practices above are recommendations for this guide.

Incident happening now? Start here

Act quickly after a suspected incident

Do not wait for certainty. Run containment, payment recovery and assessment in parallel under a named incident lead. Use an alternative trusted communication route if email may be compromised.

Employee actions

Stop the interaction and contact IT urgently. State whether you opened a link, entered credentials, approved a prompt, granted permissions, ran software, disclosed data or sent money. Preserve the original message and note the time. If software ran or remote control was granted, disconnect the affected device from networks if safe to do so. Do not wipe or restart it unless directed.

A click alone does not prove compromise, but IT should assess what followed. Do not withhold a report because the page showed an error or nothing obvious happened.

Finance actions

For suspected payment fraud, **call the bank's fraud team immediately** to request a stop or recall. Preserve the beneficiary and transaction details. Alert the finance lead, prevent further payments to the suspect destination and arrange a report to An Garda Síochána. Do not delay the bank call while assembling every detail. [8]

IT and service-provider actions

For an account compromise, assess blocking sign-in, reset credentials safely and revoke sessions. Check authentication methods, devices, app grants, administrative roles and mailbox rules or forwarding. Remove unauthorised access and investigate affected messages and files. Preserve logs and relevant evidence. [13]

Do not assume session revocation immediately ends every access token or application session. Verify containment and continue monitoring; Microsoft's device-code investigation highlights persistent-access risks. [7]

Incident lead actions

Keep a timeline, record decisions and involve the privacy lead or DPO where appointed. Assess personal data, customers, suppliers and business services affected. Check contractual and insurance notification requirements and use the applicable authority routes on page 22.

Before restoring normal work, confirm that access is secured, affected devices are assessed and critical services work. Brief affected people through trusted channels. Conduct a practical review of how the attack succeeded and assign corrective actions.

Recommended preparation

Keep the bank fraud number, IT escalation route, privacy contact, insurer contact and a deputy incident lead available offline. These steps are general guidance: follow your own incident plan and your IT provider's advice for your systems.

Separate internal and legal reporting

Do this first: tell IT straight away. If money has moved, call your bank's fraud team. If personal data may be involved, tell your privacy lead or DPO so the 72-hour clock can be assessed. **One report does not automatically satisfy every obligation.**

GDPR · personal data breach

72h
to the DPC, where feasible, from awareness

NIS2 model · significant incident (if in scope)

24h
early warning

72h
notification

1 mo
final report

GDPR and personal data

A personal data breach can involve loss, destruction, alteration, unauthorised disclosure or access. An intercepted phishing email is not automatically a personal data breach; an exposed mailbox containing personal information may be. [16]

The controller must notify the competent supervisory authority, normally the DPC for relevant Irish processing, without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to result in a risk to people's rights and freedoms. Document all personal data breaches and the assessment, including decisions not to notify. [16, 17, 18]

If high risk to individuals is likely, inform them without undue delay, subject to the applicable legal exceptions. A processor must notify its controller without undue delay; it should not treat the controller's 72-hour period as its own waiting period. Cross-border processing can affect which authority is competent. [17, 18]

NIS2 requires a scope and status check

NIS2 is not a universal rule for every SME. Sector, activity, size, group relationships and specific exceptions matter. Some entities can be covered regardless of size. A supplier may also face customer security requirements without itself being directly in scope. [19]

Position at 30 October 2026: Ireland's NCSC describes transposition as outstanding, and a 7 October 2026 parliamentary answer said the implementing Bill was being finalised, with transposition targeted by year-end. Check the current position before relying on any NIS2 deadline. [20, 21]

The Directive's model for significant incidents generally includes an early warning within 24 hours, notification within 72 hours and a final report within one month of notification, with specific exceptions and provision for ongoing incidents. This is separate from GDPR. Confirm the regime, threshold and authority that apply to your organisation. [22]

For suspected crime, contact **An Garda Síochána**. Use the NCSC's current incident-reporting route where appropriate. Neither replaces a required notification to the DPC, another regulator or a contractual partner. This page is general information, not legal advice; confirm your obligations with your DPO or legal adviser. [8, 17]

FOR MANAGEMENT ACTION TRACKER

Your first 30 days

A recommended sequence, not a statutory timetable. Name an owner, set a due date and record the evidence. Fix urgent exposure now rather than waiting for its week.

#	Action	Owner	Due	Evidence of completion	Status
	Days 1–7 Establish the essentials				
1	Publish the routine security reporting route	**Business owner**		Route circulated to all staff and contractors	☐ Done
2	Publish the urgent phone route and out-of-hours cover	**Business owner**		Tested contact sheet naming finance, IT and privacy decision-makers	☐ Done
3	Start verifying bank-detail changes independently; confirm the bank fraud contact	**Finance lead**		Approved procedure; pending changes reviewed before the next payment run	☐ Done
4	List critical accounts and devices; check MFA, alerts and leaver access	**IT owner**		Owned list of urgent gaps	☐ Done
	Days 8–14 Reduce account and device exposure				
5	Plan phishing-resistant sign-in, starting with high-impact roles	**IT provider**		Phased rollout plan with licence needs (page 19)	☐ Done
6	Review app consent, device-code use, forwarding and privileges	**IT provider**		Findings list with due dates and documented exceptions	☐ Done
7	Check updates, supported devices and recovery; agree which alerts are monitored and who contacts you	**Operations lead**		Coverage report and agreed alert contacts	☐ Done
	Days 15–21 Rehearse the decisions				
8	Run the three Decision Exercises (pages 14–16) with remote staff and new starters	**Managers**		Outcomes recorded; staff used the real reporting route	☐ Done
9	Rehearse a compromised mailbox with payment fraud: bank call, containment, evidence, reporting duties	**Incident lead**		Recorded outcome, corrected steps and named deputies	☐ Done
	Days 22–30 Demonstrate and sustain				
10	Demonstrate a safe restore of critical data; test containment steps	**IT and operations**		Restore test result and containment timings	☐ Done
11	Review open actions, NIS2 scope, reporting routes and supplier commitments; fund fixes; set the next review	**Business owner**		Signed action register with owners, dates, accepted exceptions and next review date	☐ Done

Completion of this plan improves readiness; it is not a certification of security or compliance.

Make the next step practical

Choose one process to test this week. A bank-detail change, an unexpected sign-in prompt or an urgent support request will tell you more about readiness than a general conversation about being careful.

Five questions for your next review

1. Can an employee independently verify a payment change without using information from the request?
2. Are high-impact accounts protected with appropriate authentication and secure recovery?
3. Can staff report an urgent concern when email is unavailable?
4. Does someone own investigation and containment, including outside normal hours?
5. Can the business demonstrate that critical data can be restored and that reporting obligations have been assessed?

If an answer is unclear, assign an owner and agree what evidence will resolve it, starting with the highest-impact gap.

Take it to IT.ie

Bring three things to the conversation

- Your answers to the five questions on this page.
- Your 30-day tracker (page 23), with owners and dates.
- Your IT provider's answers to the management questions on page 19.

Email us with "Social engineering guide" in the subject line and tell us which question you could not answer. We will talk through the controls in this guide with you.

hello@it.ie



A useful commitment for every team

We will make time to verify consequential requests. We will keep clear reporting routes available. We will support people who report concerns promptly and use what we learn to improve our processes.

References and evidence notes

References are numbered in the text. Web sources were checked on 30 October 2026. Source publication years and observation periods are distinct. Recommendations and fictional scenarios are editorial guidance, not additional research findings.

[1] **IT.ie. Social Engineering: A Guide to Understanding the Attacks and How to Mitigate the Risks.** Background on manipulation, impersonation, recognition and response.
it.ie/wp-content/uploads/2023/05/A-Guide-to-Social-Engineering.pdf

[2] **IT.ie. Phishing Guide 2023.** Background on business email, invoice fraud, QR codes and training.
it.ie/wp-content/uploads/2023/09/IT.ie-Phishing-Guide-2023.pdf

[3] **IT.ie and SonicWall. CyberPulse Ireland 2025.** Research by Censuswide among 1,000 office workers based in Ireland. Method summary p. 3; phishing and training pp. 6–7; remote working and device use pp. 8–9; responsibility and reporting pp. 10–11. Self-reported survey findings.
it.ie/cyberpulse-ireland-2025/

[4] **Central Bank of Ireland. Payment Fraud Statistics 2025.** Published 4 September 2026. Headline total and annual change, p. 1. Scope: reporting Irish-resident payment service providers, not Irish SMEs alone.
centralbank.ie/docs/default-source/statistics/data-and-analysis/payment-fraud-statistics/payment-fraud-statistics-2025.pdf

[5] **ENISA. ENISA Threat Landscape 2026.** Published 22 September 2026; observations from January to December 2025. See pp. 11–12 and the cybercrime analysis for social engineering, ClickFix and phishing services.
enisa.europa.eu/publications/enisa-threat-landscape-2026

[6] **CERT-EU. Threat Landscape Report 2025: A Year in Review.** Released 8 April 2026. Covers Union entities and their ecosystem; its observations are not a representative Irish SME survey.
cert.europa.eu/publications/threat-intelligence/tlr2025

[7] **Microsoft Threat Intelligence, Microsoft Defender Experts and Microsoft Security Research. Unmasking EvilTokens: Getting to the root of device code phishing.** 22 September 2026. Campaign research and mitigation guidance.
microsoft.com/en-us/security/blog/2026/09/22/unmasking-eviltokens-getting-to-the-root-of-device-code-phishing/

[8] **Irish NCSC. Protecting Against Business Email Compromise and Payment Fraud.** 25 July 2025. Definition, verification, payment controls and response.
ncsc.gov.ie/pdfs/NCSC_BEC_Guidance.pdf

[9] **Microsoft Learn. Conditional Access authentication strengths.** Method distinctions and licensing requirements.
learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strengths

[10] **Microsoft Learn. Authentication methods in Microsoft Entra ID: Passkeys FIDO2.** Service binding and user verification.
learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passkeys-fido2

[11] **Microsoft Learn. Configure how users consent to applications.** Consent restrictions and permission governance.
learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent

References and further guidance

[12] **UK NCSC. Multi-factor authentication for your corporate online services: Recommended types of MFA.** International context on the protections and limits of different methods.
ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-types-of-mfa

[13] **Microsoft Learn. Respond to a compromised email account in Microsoft 365 (Microsoft Defender for Office 365).** Account, session, permission and mailbox investigation.
learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account

[14] **Irish NCSC. Cyber security for small business.** February 2025 edition. Asset identification, updates, basic protections, MFA, backups and passwords.
ncsc.gov.ie/pdfs/NCSC-SME-Guidance-0225.pdf

[15] **Microsoft Learn. Block authentication flows with Conditional Access policy.** Device-code restrictions, exceptions and testing.
learn.microsoft.com/en-us/entra/identity/conditional-access/policy-block-authentication-flows

[16] **Data Protection Commission. What do I do if there is a security breach?** Personal-data breach definition and notification principles.
dataprotection.ie/en/faqs/responsibilities-data-controllers/what-do-i-do-if-there-security-breach

[17] **Data Protection Commission. Breach Notification.** Current reporting route, risk assessment and records. Consult the linked practical guide for notification detail.
dataprotection.ie/en/organisations/know-your-obligations/breach-notification

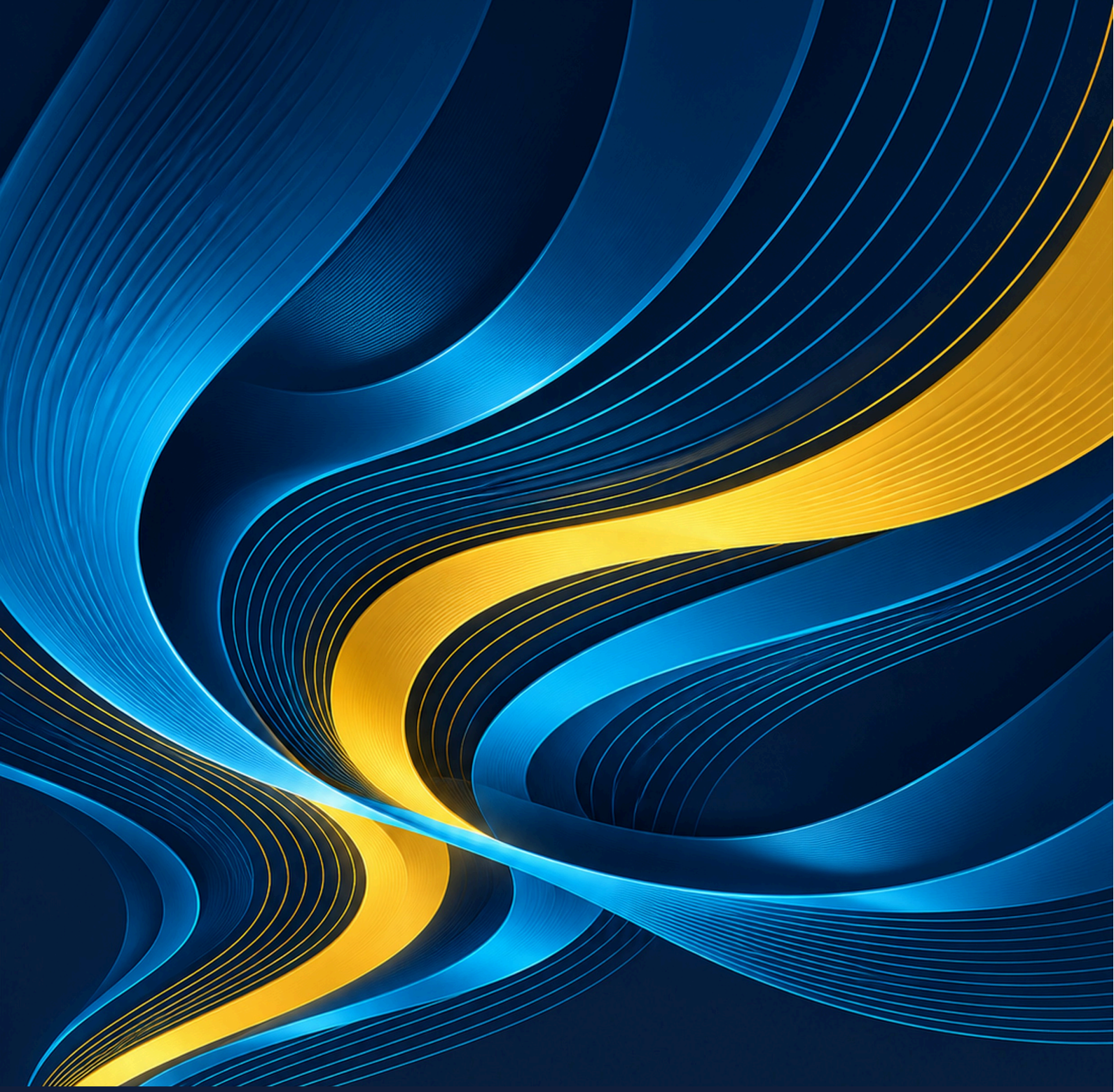
[18] **European Commission. Obligations, section on notifying data breaches; GDPR Articles 33 and 34.** Controller, processor and individual-notification requirements. DPC guidance should be read with the legal text.
commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/obligations_en
eur-lex.europa.eu/eli/reg/2016/679/oj

[19] **Irish NCSC. NIS2 FAQ.** Scope, size, group relationships, exceptions and supply-chain considerations. Awareness guidance, not a determination of an individual organisation's status.
ncsc.gov.ie/nis2/FAQ/

[20] **Irish NCSC. NIS2.** National transposition status and existing NIS arrangements. The page displays a 24 June 2025 update; read alongside the later parliamentary statement below.
ncsc.gov.ie/nis2/

[21] **Houses of the Oireachtas. Departmental Policies, written answer to Question 24, 7 October 2026.** Ministerial update on the National Cyber Security Bill and intended transposition timetable.
oireachtas.ie/en/debates/question/2026-10-07/24/

[22] **Directive EU 2022/2555, Article 23.** Significant-incident reporting model, including timing and exceptions. Check Irish implementation and applicable sector rules before relying on these requirements.
eur-lex.europa.eu/eli/dir/2022/2555/oj



Recognise. Verify. Report.

Ready to act on this guide? Email us your answers to the five review questions and your 30-day tracker.

IT.ie

hello@it.ie

it.ie