LEADERSHIP COMMENTARY / CYBERSECURITY

Stop Making Employees the Last Line of Defence

Security training matters. So does designing a workplace in which one mistake need not become a crisis.

Jennifer Oriwoh

An employee receives an urgent request that appears to come from a senior colleague. The message concerns a payment, arrives during a busy afternoon and sounds plausible. In this hypothetical case, the employee acts before checking it independently.

The easy response is another reminder to be vigilant. The more useful response examines why an unverified message could move money, which account permissions made the action possible and how quickly the organisation could detect and reverse it.

Staff judgment belongs in a security programme. It should not have to compensate for every weakness in the surrounding process.

Give caution a workable process

The UK National Cyber Security Centre's guidance on spotting cyber attacks describes phishing through emails, texts and calls that pressure people into disclosing information or transferring money. It advises verifying doubtful messages through independently obtained contact details. That is practical advice; it becomes more useful when the business makes it easy to follow.

For a payment change, the process should explain who verifies the request, which trusted contact route to use and what happens when the requester cannot be reached. Finding a phone number inside the suspicious message defeats the purpose. So does a workplace in which delaying an executive's request is treated as disobedience.

The control also needs to survive a busy day. A procedure that requires lengthy investigation for every routine transaction is likely to create queues and workarounds. Reserve stronger checks for consequential changes, make the verification route clear and give staff authority to pause an uncertain request.

Training can then use the actual workflow rather than a generic warning about suspicious spelling. The relevant lesson is how to respond to a plausible request under pressure, including when a familiar-looking sender is insufficient evidence.

Protect accounts as well as attention

Account security provides another layer. The NCSC's guidance on recommended authentication methods prioritises FIDO2 credentials where appropriate and distinguishes their phishing resistance from weaker methods. Its recommendations consider the available devices and the organisation's requirements. Not every form of multi-factor authentication provides the same protection.

A business should therefore check which methods its important services actually support, how administrators enrol users and how a lost device is handled. Enabling a stronger login while leaving recovery poorly controlled can undermine the intended protection. Staff also need a usable route back into their accounts.

Access should reflect the task. A person who needs to read a customer record may not need to export every record or change payment details. Reducing unnecessary permissions cannot prevent every incident, but it can reduce what a compromised account is able to do. The permissions review should include people who have changed roles or left.

These decisions require cooperation between operations and technical staff. A security setting that blocks a legitimate task without a supported alternative can encourage people to move the work into less controlled channels.

Prepare to recover without improvising

Prevention will never answer every operational question. If staff lose access to important records, the business needs to know what can be restored and who can authorise the recovery.

NCSC backup guidance recommends copying the data an organisation needs to operate, protecting those copies and knowing how to restore them. A completed backup notification is a useful signal, but a restore exercise provides different evidence: whether the records can be recovered and used.

A proportionate rehearsal can restore permitted test data into an isolated destination, confirm that important files are present and record the steps that were unclear. It should not overwrite live work merely to prove that a backup exists. The result can inform realistic expectations about disruption without pretending that a small rehearsal certifies the whole recovery plan.

Reporting is part of recovery too. Someone who realises they may have approved a fraudulent request should know where to report it immediately. If the predictable response is humiliation, the organisation risks making early disclosure harder. Managers should distinguish a deliberate breach of rules from an honest report of a mistake.

The purpose of these measures is to give vigilance support: a verification route, stronger account protection, limited authority and a practiced response. A business that wants careful staff should build conditions in which being careful is possible, and in which a lapse can be contained.

Sources

NCSC, Spotting cyber attacks.

NCSC, Recommended types of MFA.

NCSC, Backing up your data.