

Trust is important.
Verification is essential.

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: **net-defence.com**

Why this matters

Cybercriminals increasingly target people, not technology. Rather than breaking into systems, they impersonate trusted individuals using email, phone calls, text messages, WhatsApp, Teams, and other communication platforms. Their objective is simple: create urgency, exploit trust, and persuade someone to take action before stopping to verify.

We can deploy filtering, anti-spoofing, malware protection, and threat detection to email platforms. We cannot deploy the same level of control to every text message, WhatsApp conversation, Teams chat, or phone call. As communication channels continue to expand, culture becomes an increasingly important security control. When technology cannot verify the request, people must.

Within the Ogilvie Group and that of our customers, we are seeing real examples of attempted fraud and impersonation attacks. These attacks are rarely sophisticated from a technical perspective. Instead, they rely on something much simpler: uncertainty.

The scenario

- An employee receives a message that appears to come from a director.
- A payment request suddenly becomes urgent.
- An established process is bypassed to "save time".
- A colleague is pressured into acting quickly rather than checking carefully.
- The criminal succeeds not because the technology failed, but because trust was exploited.

Why criminals are focusing on impersonation

Modern fraudsters understand that people are busy. They also understand how people make decisions. When a request appears to come from a trusted source, most people naturally want to be helpful and responsive. Criminals exploit this by creating a sense of familiarity before making their request.

A common technique is to create a WhatsApp profile using a publicly available photograph taken from a company website, LinkedIn profile, or social media account. Within minutes, an attacker can create an account that visually appears to belong to a director or senior leader.

The photograph itself becomes part of the deception. When employees see a familiar image alongside a familiar name, they can unconsciously assume the message is genuine before considering whether it has been verified. This is known as familiarity bias; our brains naturally place greater trust in things we recognise. The attacker's objective is not to defeat technology. The attacker's objective is to bypass critical thinking long enough for somebody to act.

The UK Government's national assessment of fraud identifies impersonation-based frauds, including payment diversion fraud, as some of the most harmful forms of fraud affecting UK organisations and individuals. Criminals deliberately position themselves between trusted parties and exploit authority and urgency. Recent assessments also highlight the increasing use of AI and emerging technologies to support fraud and impersonation activity.

The message is clear: technology remains important, but people remain the primary target.

Continued...

The power of "I will never..."

One of the most effective ways to reduce this risk is to remove uncertainty altogether. The "I will never..." pledge creates clear and memorable boundaries around how leaders will and will not communicate with their teams. This includes simple commitments such as:

- I will never ask you to purchase gift cards or vouchers.
- I will never ask you to share passwords or MFA codes.
- I will never ask you to bypass our established processes because something is urgent.
- I will never communicate company business through unofficial channels.

These statements are intentionally simple. That is because simple rules are easier to remember, easier to recognise, and easier to apply under pressure. Over time, repeated behaviours become habits. Habits become unconscious actions.

Eventually, employees no longer need to analyse every suspicious request in detail. They instinctively recognise when something falls outside the agreed rules and know it needs to be verified. That is where culture becomes one of the strongest security controls available to any organisation.

Verification is not distrust

One of the greatest challenges an organisation faces is that employees can sometimes worry about questioning senior colleagues or appearing difficult. That concern plays directly into the hands of cyber criminals.

Verification should never be viewed as distrust. It should be viewed as professionalism. A quick phone call, Teams message, or face-to-face conversation can prevent a costly mistake, protect a colleague, and potentially stop a fraud before it occurs. We should never be concerned about inconveniencing a colleague by verifying a request.

I would far rather someone makes a quick phone call to confirm something than see a team member or business become the victim of fraud.

Why a no-blame culture matters

No organisation can eliminate every mistake. The goal is not perfection. The goal is early detection, rapid reporting, and continual improvement.

- People should feel comfortable speaking up when something doesn't feel right.
- People should feel comfortable reporting suspicious activity.
- People should feel comfortable admitting a mistake quickly so the organisation can respond and minimise any impact.
- If somebody questions a genuine request, thank you.
- If somebody reports something suspicious, thank you.
- If somebody makes a mistake and tells us quickly, thank you.

The strongest security cultures are not the ones that experience no incidents. They are the ones where people feel confident enough to report concerns without fear of criticism or blame. When people feel safe to raise a concern, organisations learn faster, respond faster, and become more resilient.

Continued...

Security is a culture, not just a technology

Businesses invest heavily in firewalls, endpoint protection, monitoring platforms, and cyber-security controls. These are all important. However, one of the most effective controls costs nothing. Clear leadership, clear expectations, permission to verify, and a culture where questioning unusual requests is actively encouraged.

By making the "I will never..." promise today, we remove one of the key tools criminals rely upon: uncertainty. The clearer we are about what we will and will not ask of our colleagues, the harder it becomes for fraudsters to exploit trust and the lower our collective risk becomes.

- Criminals can spoof an email address.
- They can fake a phone number.
- They can increasingly imitate a voice.
- What they cannot easily defeat is a culture where everyone has permission to stop, check, and verify.

Trust is important. Verification is essential. Stop. Check. Verify.