SECURITY

Fraud Can Start with a Believable Message

An attempted fraud can begin without exploiting a software flaw. Someone poses as a supplier, a bank or a relative, uses details that make the message believable and requests urgent action. A review needs to cover technical access and the decisions people make in response.

It works because it leans on hurry and on hierarchy. A message that looks like it came from the owner, at six on a Friday, asking for an exceptional payment, is rarely questioned.

The Three Doors We Check First

- The email and phone number that recover everything else. If someone gets in there, the rest falls in order.
- Who may authorise a payment, and with what confirmation outside the channel where it was requested.
- What public information about you and your family makes a believable message easy to build.

Verifying Is Not Distrust

The rule that pays off most is also the dullest. Every request for money or access is confirmed through a second channel agreed in advance. Always, with no exception for rank or urgency. Once the exception exists, all the attacker has to do is manufacture urgency.

It is worth rehearsing before you need it. A short call to the usual number. An agreed phrase. A second pair of eyes above a certain amount. These are agreements, not software.

What Executive Protection Covers

We review the accounts and devices of whoever decides and, if agreed, of their family. We strengthen access and recovery, cut the public exposure that serves no purpose, and write down what to do when something is lost or someone leaves the company.

> *These measures reduce risk and shorten detection. None removes the possibility of fraud, and anyone*

promising otherwise deserves a second look.

A Check You Can Run

A rehearsal could use a fictional supplier asking for new bank details to be used on an invoice. The person processing it should contact the supplier through previously verified details, rather than the number in the request. Record who confirms the change and who approves it. This exercises the decision without sending money or testing a real customer.

Supporting guidance: FTC guidance on verifying suspicious messages.
https://consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams

Continue with: The Email That Recovers Your Accounts Needs a Way Back In.
https://systems.kavaliero.com/en/blog/the-email-that-recovers-all-your-accounts

For help with this work, see the scope of Executive Digital Protection.
https://systems.kavaliero.com/en/services/executive-security