

■ SECURITY

Fraud Almost Never Starts with a Hack

The picture of an attacker breaking a system is comfortable, because it leaves the problem on the technology side. What we see is almost always simpler. Someone writes posing as a supplier, as the bank or as a relative, with enough detail to sound real, and asks for something urgent.

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.