

A TWO-MINUTE FIELD GUIDE FOR BUSINESS OWNERS

The attack rarely looks like an attack.

A camera recorder. A familiar-looking web address. An unexpected VPN login. These ordinary details can be the first visible signs of a much larger problem.

WHAT WE HAVE ENCOUNTERED

01 The DVR that became a launch point

Softfusion discovered a compromised DVR with an altered web server that was being used to target other offices. The lesson: devices outside the usual laptop inventory need attention, too.

02 The domain that looked almost right

We identified domains registered to resemble a customer's domain. A lookalike can create an opportunity for impersonation; its registration alone does not prove an attack is underway.

03 The suspicious way in

We have seen suspicious VPN login activity aimed at network resources, received alerts, and terminated the connection. Unfamiliar access deserves prompt investigation, even when a login appears legitimate.

DETECT / INVESTIGATE / CONTAIN

Field Effect MDR can monitor endpoint behavior, cloud activity, and - in the appropriate package with network monitoring deployed - traffic from devices such as cameras and recorders. A protected endpoint showing signs of compromise can be isolated, according to the response settings and investigation.

Softfusion Cyber combines these tools with our team to review the signals, communicate what matters, and coordinate the response.

Next page > The practical do's and don'ts

THE PRACTICAL CHECKLIST

Six habits that close common gaps.

Share this page with whoever manages your computers, email, remote access, and business devices.

01 KNOW EVERY DEVICE

DO: Include cameras, DVRs, printers, servers, and vendor-installed equipment in your inventory.

DON'T: Assume a device is harmless because nobody uses it like a PC.

02 GUARD REMOTE ACCESS

DO: Require MFA for VPN and administrative access; review unusual sign-ins promptly.

DON'T: Leave old accounts, shared credentials, or unused VPN access in place.

03 VERIFY THE SENDER

DO: Confirm changed payment instructions or urgent requests using a known phone number.

DON'T: Trust a familiar display name or a web address that merely looks close.

04 CONTROL REMOTE TOOLS

DO: Keep an approved list of remote administration software and investigate surprises.

DON'T: Let unrecognized tools remain installed without an owner or explanation.

05 PREPARE TO CONTAIN

DO: Agree in advance who can isolate a computer and how your team will continue working.

DON'T: Wait for an incident to decide who has authority to act.

06 PRACTICE RECOVERY

DO: Patch promptly, keep tested backups, and teach staff how to report suspicious activity.

DON'T: Treat monitoring as a replacement for these basics.

WANT TO KNOW WHAT YOUR CURRENT COVERAGE MISSES?

Reply to your Softfusion contact and ask for a 20-minute security review.

Sources: CISA Secure Your Business | Field Effect MDR product & support documentation