

First Hour

Cyber Incident Response for Small Business

Print this. Keep it where the designated responders can grab it fast.

PHISHING CLICK

Someone typed a password into a fake login page. Assume the attacker is already in the mailbox.

- From a CLEAN device: reset the user's password in Microsoft 365 or Google Workspace.
- Sign the account out of all active sessions.
- Reset MFA registrations entirely and force re-enrollment on every device.
- Screenshot ALL inbox rules (evidence), then delete every one, not just what looks suspicious.
- Check transport rules at the Exchange/Workspace admin level too, not just user rules.
- Review recent OAuth grants (M365: Entra ID > Enterprise apps > User consented apps; Workspace: Security > API controls); consent phishing survives password resets.
- Search last 48 hours of sent mail; warn anyone emailed about invoices or vendor banking.
- If the password was reused elsewhere (bank, personal email, password manager), reset those too.

FRAUDULENT WIRE

Money went to the wrong account. The FBI Financial Fraud Kill Chain (via FinCEN RRT) can recall wires still in a US bank within roughly 72 hours.

- BEFORE YOU CALL, gather: wire date/time and amount; your bank name and account number; receiving bank name, address, and SWIFT (international) or routing (domestic); beneficiary name and account number; transaction confirmation number; short fraud narrative.
- Call the bank's fraud line; request a SWIFT recall.
- File at IC3.gov with the wire details.
- Call your FBI field office; ask for the cyber squad.
- Then notify your cyber insurance carrier.

RANSOMWARE

A ransom note is on the screen. Treat the whole network as compromised, not just this one machine.

- Unplug the machine's network cable, turn wifi off, LEAVE IT ON. Memory holds evidence.
- Photograph the ransom note.
- Do NOT run antivirus, decrypt, or clean up. Every action destroys evidence.
- Isolate other endpoints, especially servers and the domain controller.
- Do NOT log in from other machines; that spreads credentials the attacker is watching for.
- Change all admin passwords from a known-clean device.
- Check backups from an unaffected device (a phone or a laptop off the network); attackers routinely destroy backups before triggering the encryption.
- Call cyber insurance FIRST, before your own IT provider. Most SMB policies require pre-approved vendors; self-remediation voids coverage.

PHONE NUMBERS TO HAVE READY

Fill these in now. If you're reading this during an incident, you're too late for this part.

CYBER INSURANCE 24-hour claims line, in your policy PDF	BANK FRAUD your bank's fraud line
IT PROVIDER after-hours line	FBI FIELD OFFICE find yours at fbi.gov/contact-us