TOOLKIT GUIDE
English

ZERODAY TECH LABS

Incident Response and Recovery Checklist

What to do first after a suspected malware infection, account exposure, or scam.

Audience	Families dealing with a suspicious event or recent mistake.
Purpose	Give calm recovery steps and reduce additional harm.
Best use	Use from a clean device when possible.

Do this first

[ ]	Disconnect the suspicious device from the internet if needed.
[ ]	Do not enter new passwords on a device that may be compromised.
[ ]	From a clean device, change the email password first.
[ ]	Enable multifactor authentication.
[ ]	Check recent logins and sign out of unknown sessions.
[ ]	Call the bank or card issuer if money or payment data may be involved.

Clean and recover

[ ]	Run a built in security scan.
[ ]	Apply updates.
[ ]	Remove suspicious apps or browser extensions.
[ ]	Restore files from backup if needed.
[ ]	Save screenshots and notes for reporting.

Do not do this

[ ]	Do not share codes with a caller.
[ ]	Do not allow remote access because a pop up told you to.
[ ]	Do not pay a stranger who claims they can remove a virus.

Keep this guide near the device or account it protects. Small habits make a real difference when they are repeated.