

Pause. Verify. Report.

A practical response guide to keep nearby. Course edition 2026.1.

Use the reporting contact supplied by your company. If you do not have it, use your established IT or supervisor contact from a trusted directory.

Before you act

Check the request, not just the appearance. Verify unexpected sign-ins, access requests, sensitive disclosures, and payment changes through a contact or application you already trust. Do not use the replacement number or link in the message.

If you only clicked

Stop interacting. Close the page and report the message. Tell IT when you clicked, which device you used, and whether anything downloaded. Do not reopen it to investigate.

If you entered information or approved access

Contact IT immediately through a trusted channel. Describe whether you entered a password, shared a code, approved MFA, or granted app permissions. Secure the account through the official service on a known-safe device; IT may need to revoke sessions and app access.

If you ran a file or installed software

Stop sensitive work and contact IT, using a separate trusted device if possible. Follow approved containment instructions. Do not alter, power down, or disconnect operational or safety-critical systems on your own; involve the operations lead.

If you sent money or sensitive information

Contact IT and the responsible manager immediately. Involve the payment team and bank through known channels if money moved. Preserve the messages and transaction references as directed. Do not pay another fee or negotiate with the sender.

What to include in your report

Approximate time; message subject; device; what you clicked, opened, entered, or approved. Describe the type of information shared. Never include an actual password, MFA code, recovery code, or operational access code.

For immediate physical-safety concerns, follow your established emergency plan. This guide supports, but does not replace, company incident and operational procedures. © 2026 Shiner Ops. learn.shinerops.com