



Access & Redirection Scams

Responding to Scams with Deceptive Redirections

Access & redirection scams occur when criminals trick you into visiting a fake website or taking action through deceptive links or codes. These sites are designed to steal logins, payment details, or install malware, often while appearing legitimate.

This guide applies to:

- QR code scams
- Phishing-linked payment pages
- Fake login portals
- Redirect scams (being silently sent to a different site)

If you interacted with a suspicious link or code, act immediately. Speed limits damage.

Access & Redirection – Do This First

Preserve Evidence

Before clearing anything:

- Screenshot or save:
 - The URL (full address)
 - The page content
 - QR code image (if used)
 - Messages or emails that led you there
- Record:
 - Date and time
 - How you arrived (email, text, ad, poster)
 - What the page asked you to do
- Documentation supports reporting and recovery.

Stop and Exit Immediately

If you suspect a fake site or redirect:

- Close the browser or app
- Do not submit information
- Do not continue clicking
- Do not download anything





Do not try to “check” the site further, every click increases risk.

Verify Through a Trusted Path

If the page claimed to be from a real organization:

- Open a new browser window
- Type the official website address yourself
- Log in only from the official site or app
- Contact the organization using a known, official number

Never use contact details provided on the suspicious page.

Common Scam Types & What to Do

QR Code Scams

Signs:

- Malicious QR codes on posters, menus, parking meters, emails, or packages
- Code leads to fake payment or login pages

What to Do:

- Do not scan unknown QR codes
- If scanned, exit immediately and follow containment steps
- Report the location or platform where the QR code appeared

Phishing-Linked Payment Pages

Signs:

- Urgent payment demands
- Slightly misspelled brand names
- Requests for gift cards, crypto, or unusual payment methods

What to Do:

- Do not pay
- Verify charges directly via official accounts
- Contact your bank if any details were entered

Fake Login Portals

Signs:

- Unexpected login prompts





- “Session expired” messages from links
- Login pages that look right but have odd URLs

What to Do:

- Exit immediately
- Change passwords from a safe device if you entered credentials
- Watch for login alerts

Redirect Scams

Signs:

- Clicking a link sends you to a different site than expected
- Often used in ads, shortened links, or compromised websites

What to Do:

- Close the page
- Do not proceed
- Scan the device if downloads occurred

If You Entered Information or Took Action

Secure Accounts Immediately (From a Safe Device)

If you entered:

- Passwords or codes - Change passwords immediately
- Payment details - Contact your bank or card issuer
- Personal information - Monitor for identity misuse
- Log out of all sessions and update recovery settings.

Check the Device

If a file downloaded or a prompt appeared:

- Disconnect from Wi-Fi and networks
- Run a reputable security scan
- If unsure, seek professional IT help before continuing to use the device

Improper handling can hide infections.





Report the Scam

Report to the Platform

- Email provider, messaging app, or social network where the link appeared
- Website or business impersonated
- Location owner (for physical QR codes)

Additional Reporting

- National Reporting
 - Federal Trade Commission (FTC)
 - Main federal agency for consumer fraud
 - reportfraud.ftc.gov
 - Internet Crime Complaint Center (IC3) – FBI
 - Tracks internet-based financial crimes and scams
 - ic3.gov
 - U.S. Postal Inspection Service
 - If the scam involved mailed checks, money orders, or parcels
 - uspis.gov/report
 - Secret Service Cleveland Field Office
 - Main federal agency for financial crimes
 - 216-750-2058
- Ohio Resources
 - Ohio Attorney General – Consumer Protection & Identity Theft
 - <https://www.ohioattorneygeneral.gov>
 - Consumer Protection Hotline: 800-282-0515
- Geauga County
 - Geauga County Sheriff's Office
 - <https://www.geaugasheriff.org>
 - Local police non-emergency line for documentation
 - Call 911 if threats, coercion, or immediate danger are involved

Recovery – After a Redirection Incident

- Monitor accounts and statements closely for several weeks
- Watch for follow-up scams referencing the incident
- Keep all reports, screenshots, and case numbers together
- Revisit account security and privacy settings
- Redirect scams often lead to secondary attacks.





How to Reduce Access & Redirection Scam Risk

- Treat unexpected links and QR codes as suspicious
- Slow down, urgency is the scammer's tool
- Check URLs carefully before entering information
- Use official apps or typed-in addresses instead of links
- Ask for a second opinion before acting under pressure
- Add a Trusted Contact to all financial accounts

