



Phishing

Responding to Phishing

Phishing is a type of online scam where criminals send fraudulent emails (or messages) designed to trick you into clicking a link, opening an attachment, or sharing sensitive information such as passwords, financial details, or verification codes.

Phishing emails often pretend to be from:

- Banks or credit card companies
- Online retailers or delivery services
- Employers, schools, or coworkers
- Government agencies
- Tech companies (email providers, cloud storage, streaming services)

Phishing is one of the most common entry points for account compromise, malware infections, identity theft, and financial fraud.

Common Signs of a Phishing Email

Be cautious if an email:

- Creates urgency or fear (“Act now,” “Account suspended”)
- Asks you to verify, reset, or confirm information unexpectedly
- Contains links or attachments you weren’t expecting
- Errors can be a sign, but polished messages can still be scams, but polished messages can still be scams.
- Uses a sender address that looks “almost right”
- Pressures you to bypass normal procedures
- Asks for passwords, codes, gift cards, or payment

If something feels off, trust that instinct.

Phishing – Do This First

Do Not Interact Further

If you suspect an email is phishing:

- Do not click links
- Do not open attachments
- Do not reply
- Do not forward to friends; if your workplace or provider has a phishing-reporting process, use that

Interacting confirms your address is active and may increase targeting.





Preserve Evidence (If necessary)

Before deleting or reporting the email:

- Take screenshots if needed
- Note:
 - Sender address
 - Subject line
 - Date and time
 - What the email asked you to do

Verify Through a Separate Channel

If the email claims to be from a real organization:

- Go directly to the organization's official website (do not use the link)
- Contact them using a known phone number or app
- Confirm whether the message is legitimate

If You Clicked a Link or Opened an Attachment

Stop and Contain

- If a file ran, a prompt installed software, or the device behaves oddly, disconnect from Wi-Fi and networks
- Do not log into any accounts
- Do not continue clicking or entering information

Secure Accounts Immediately (From a Safe Device)

If you entered credentials or codes:

- Change passwords for the affected account immediately
- Change passwords for any other accounts using the same or similar password
- Watch for password reset or login alerts

Scan the Device

- Run a full security scan using reputable antivirus or antimalware software
- If you are not confident performing scans safely, seek expert help
- Improper handling can worsen damage or hide infections.

If You Shared Personal or Financial Information

Act quickly if you shared:

- Passwords or verification codes
- Bank or credit card details





- Social Security number or personal data

Steps to take:

- Contact your bank or financial institution immediately
- Monitor accounts for suspicious activity
- Follow guidance from the organization involved
- Consider placing a fraud alert if advised

Report the Phishing Attempt

Report to Your Email Provider

Most email services allow you to:

- Mark the message as “Phishing” or “Scam”
- This helps protect others

Additional Reporting

- National Reporting
 - FBI Internet Crime Complaint Center (IC3)
 - <https://www.ic3.gov>
 - (Especially important if money, data, or accounts were affected)
 - Federal Trade Commission (FTC) - report consumer fraud and scams at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud).
- Ohio Resources
 - Ohio Attorney General – Consumer Protection & Cybercrime
 - <https://www.ohioattorneygeneral.gov>
 - Hotline: 800-282-0515
- Geauga County
 - Geauga County Sheriff’s Office
 - <https://www.geaugasheriff.org>
 - Local police non-emergency line if fraud or identity theft occurred
 - Call 911 if threats or immediate danger are involved

Recovery – After a Phishing Incident

- Monitor email and accounts closely for several weeks
- Watch for follow-up scams referencing the incident
- Review account security and recovery options
- Be extra cautious of “help” emails claiming to fix the problem
- Phishers often follow up once they know someone clicked.





How to Reduce Phishing Risk

- Slow down, urgency is a scam tactic
- Treat unexpected emails as suspicious by default
- Verify before trusting, especially with money or access
- Ask for help early, second opinions prevent mistakes
- Remember: legitimate organizations do not pressure you to act quickly

