RESOURCE 07 | DON'T CLICK YET COMPANION RESOURCE

# Incident Evidence Log

*Companion resource for Don’t Click Yet. Referenced on page 202.*

**Purpose:** Keep a calm record of what happened, when it happened, and what evidence you preserved.
**Storage reminder:** If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

Use this log if something suspicious has happened or may have happened.

You may have clicked a link, shared a password, entered a verification code, sent money, allowed remote access, noticed a strange transaction, lost a device, received a threatening message, or discovered an account change you did not make.

This log helps you preserve details while they are still fresh.

Do not delete messages, emails, receipts, call logs, screenshots, or transaction records until you understand whether they may be useful. Evidence can help banks, payment services, account providers, law enforcement, fraud-reporting agencies, technical helpers, or trusted family members understand what happened.

This worksheet is not a substitute for calling your bank, card issuer, payment service, account provider, employer, school, or emergency services when immediate action is needed. If money, identity, safety, work data, or sensitive information is involved, act promptly through trusted channels.

## Basic Incident Information

**Date incident started or was discovered:**

**Approximate time:**

**Person affected:**

**Person completing this log:**

**Type of incident:**

- Suspicious link clicked
- Password shared or entered on suspicious site
- Verification code shared
- Bank or card issue
- Payment app issue
- Gift card scam
- Wire transfer or cryptocurrency request
- Fake family emergency
- Fake tech support
- Remote access allowed


© 2026 Click Giraffe

- Computer pop-up warning
- Suspicious email
- Suspicious text message
- Suspicious phone call
- Social media account issue
- Email account issue
- Lost or stolen phone
- Lost or stolen computer
- Identity theft concern
- Business or client data concern
- Other: _____

**Brief description of what happened:**

## Immediate Safety Questions

Answer these as soon as possible. They will help decide what to do first.

**Was money sent, charged, transferred, or requested?**

[ ] Yes
[ ] No
[ ] Not sure

**Was a password shared, typed, or possibly exposed?**

[ ] Yes
[ ] No
[ ] Not sure

**Was a verification code shared, typed, forwarded, or approved?**

[ ] Yes
[ ] No
[ ] Not sure

**Did someone have remote access to a computer, phone, or tablet?**

[ ] Yes
[ ] No
[ ] Not sure

**Was financial information entered or visible?**

[ ] Yes
[ ] No
[ ] Not sure


© 2026 Click Giraffe

**Was personal information shared?**

[ ] Yes
[ ] No
[ ] Not sure

Examples: Social Security number, date of birth, address, identity document, insurance information, medical information.

**Was a work, school, client, patient, donor, or business account involved?**

[ ] Yes
[ ] No
[ ] Not sure

**Is the affected device still connected to the internet?**

[ ] Yes
[ ] No
[ ] Not sure
[ ] Not applicable

**Has a bank, card issuer, payment service, or account provider already been contacted?**

[ ] Yes
[ ] No
[ ] Not yet
[ ] Not applicable

## Timeline

Write down the sequence of events as clearly as you can. Do not worry if you cannot remember everything. Record what you know.

| Date | Time | What Happened | Notes or Evidence |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Additional timeline notes:


© 2026 Click Giraffe

**How the Contact Started**

**How did the suspicious contact begin?**

- Text message
- Email
- Phone call
- Voicemail
- Social media message
- Messaging app
- Website pop-up
- Search result
- Online advertisement
- Marketplace message
- Dating app or social platform
- Mail letter
- In-person conversation
- Other: _____

**What did the sender or caller claim?**

- Bank problem
- Suspicious transaction
- Locked account
- Delivery problem
- Family emergency
- Computer infection
- Refund
- Prize or grant
- Government issue
- Legal issue
- Tax issue
- Subscription problem
- Job or business opportunity
- Marketplace purchase or sale
- Romance or friendship request
- Other: _____

**Exact wording or summary of the message or call:**

## Sender, Caller, or Website Details

Record every detail you have. Do not click suspicious links again just to complete this form.

**Phone number used by caller or sender:**

**Email address used by sender:**


© 2026 Click Giraffe

**Display name used:**

**Username or profile name:**

**Website or link shown:**

**Company, agency, bank, or person they claimed to represent:**

**Case number, badge number, employee number, or reference number they gave:**

**Payment recipient name, username, phone number, email, or account:**

**Other identifying details:**

### What They Asked You To Do

Check everything that applies.

- Click a link
- Open an attachment
- Sign in to an account
- Enter a password
- Share a verification code
- Approve a login prompt
- Call a phone number
- Download software
- Install remote access software
- Allow screen sharing
- Open a bank account or payment app
- Send money
- Buy gift cards
- Read gift card numbers
- Send cryptocurrency
- Wire money
- Use a payment app
- Move money “for safety”


© 2026 Click Giraffe

- Provide identity information
- Provide insurance or medical information
- Provide a photo of an ID
- Keep the situation secret
- Not call anyone else
- Other: _____

**Additional details about the request:**

**What You Did**

Be honest and specific. This section helps determine the correct recovery steps.

**Did you click a link?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, what happened after you clicked?

**Did you enter a username or password?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, which account?

**Was that password reused anywhere else?**

[ ] Yes
[ ] No
[ ] Not sure

**Did you enter or share a verification code?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, which company or account sent the code?


© 2026 Click Giraffe

**Did you approve a sign-in prompt?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, for which account?

**Did you download or install anything?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, what was the name of the file, app, or program?

**Did someone access your device remotely?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, how long did access last?

**Did you send money or provide payment information?**

[ ] Yes
[ ] No
[ ] Not sure

If yes, complete the payment section below.

## Payment or Financial Information

Complete this section if money was sent, requested, charged, transferred, or exposed.

**Payment method involved:**

- Credit card
- Debit card
- Bank transfer
- Wire transfer
- Payment app
- Zelle
- PayPal
- Venmo
- Cash App


© 2026 Click Giraffe

- Apple Cash
- Google Pay
- Gift card
- Cryptocurrency
- Check
- Cash
- Other: _____

**Amount:**

**Date and time of payment:**

**Recipient name or account:**

**Transaction ID or receipt number:**

**Bank, card issuer, or payment service involved:**

**Was the transaction reported to the bank, card issuer, or payment service?**

[ ] Yes
[ ] No
[ ] Not yet

**Date reported:**

**Case or claim number:**

**Representative name or ID, if provided:**

**Instructions given by bank, card issuer, or payment service:**


© 2026 Click Giraffe

## Accounts That May Be Affected

Check accounts that may have been exposed, accessed, used, or mentioned.

- Main email
- Bank
- Credit card
- Payment app
- Password manager
- Phone provider
- Apple account
- Google account
- Microsoft account
- Cloud storage
- Social media
- Shopping account
- Health portal
- Insurance account
- Tax or government account
- Business email
- Business banking
- Client account or portal
- Employer or school account
- Other: _____

**Account names or providers involved:**

**Actions already taken:**

- Password changed
- MFA turned on
- MFA reviewed
- Unknown devices signed out
- Recovery information reviewed
- Bank or provider contacted
- Account locked
- Account recovered
- Payment disputed
- Device disconnected
- Device reviewed
- Evidence saved
- Report filed
- Trusted person contacted
- Other: _____

**Notes:**


© 2026 Click Giraffe

## Device Information

Complete this section if a phone, computer, tablet, or other device may be involved.

**Device type:**

- Phone
- Laptop
- Desktop computer
- Tablet
- Router
- Printer
- Smart device
- Other: _____

**Device brand and model:**

**Operating system, if known:**

**Was remote access allowed?**

[ ] Yes
[ ] No
[ ] Not sure

**Remote access tool or app name, if known:**

**Was the device disconnected from the internet?**

[ ] Yes
[ ] No
[ ] Not yet
[ ] Not applicable

**Was the device used for banking, email, or password changes after the incident?**

[ ] Yes
[ ] No
[ ] Not sure

**Has the device been reviewed by a trusted person or professional?**

[ ] Yes
[ ] No
[ ] Not yet
[ ] Not needed


© 2026 Click Giraffe

**Notes:**

## Personal or Identity Information Possibly Shared

Check anything that may have been shared, exposed, uploaded, or visible.

- Full name
- Home address
- Email address
- Phone number
- Date of birth
- Social Security number
- Tax identification number
- Driver’s license
- Passport
- Bank account number
- Credit card number
- Insurance information
- Medical information
- Login credentials
- Signature
- Photo of ID
- Employer information
- Client information
- Family information
- Other: _____

**Details:**

## Evidence Saved

Check what has been saved.

- Screenshots of messages
- Screenshots of website
- Screenshots of transactions
- Emails
- Text messages
- Social media messages
- Voicemails
- Call logs
- Receipts
- Gift card photos or receipts
- Payment confirmation
- Shipping information
- Usernames or profiles
- Website addresses
- Phone numbers


© 2026 Click Giraffe

- Case numbers
- Notes from calls
- Photos of pop-up warning
- Remote access program name
- Other: _____

**Where the evidence is stored:**

**Who has access to the evidence folder:**

## People or Organizations Contacted

Record every contact you make.

| Date | Person or Organization | Phone / Website / App Used | Reason for Contact | Case Number | Next Step |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Additional notes:

## Reports Filed

Check reports that apply.

- Bank or card issuer report
- Payment app report
- Email provider report
- Phone provider report
- Social media platform report
- Marketplace platform report
- Company impersonation report
- Employer or school report
- Local police report
- Fraud report
- Identity theft report
- Internet crime report
- Insurance report
- Other: _____


© 2026 Click Giraffe

**Report location or agency:**

**Date filed:**

**Report or case number:**

**Follow-up instructions:**

## Follow-Up Scams Watchlist

After a scam, be cautious of anyone who contacts you unexpectedly claiming they can recover money, fix your computer, investigate the case, provide a refund, or represent an agency.

**Have there been follow-up calls, emails, or messages?**

[ ] Yes
[ ] No
[ ] Not sure

**Details:**

**How I verified or responded:**

## Next Steps

Use this section to list what still needs to be done.

- Contact bank or card issuer.
- Contact payment service.
- Change exposed password.
- Change reused passwords.
- Review main email account.
- Review bank account.
- Review payment app.
- Review password manager.
- Review phone provider account.
- Review cloud storage.


© 2026 Click Giraffe

- Review social media accounts.
- Turn on MFA.
- Save backup codes.
- Disconnect affected device.
- Have device reviewed.
- Report suspicious message or account.
- File fraud or identity theft report.
- Tell trusted family member.
- Monitor accounts.
- Watch for follow-up scams.
- Other: _____

**Priority next step:**

**Who will do it:**

**By when:**

## Recovery Notes

Use this space to record what was resolved, what remains uncertain, and what should be reviewed later.

## Lessons Learned

After the immediate situation is under control, write down what should change.

**What warning signs were present?**

**What helped?**

**What made the situation harder?**


© 2026 Click Giraffe

**What should be changed to reduce risk next time?**

**Family, account, device, or backup plan updates needed:**

## Final Reminder

The purpose of this log is not to blame anyone.

It is to preserve facts, reduce confusion, support recovery, and make the next step clearer.

Do not let embarrassment erase useful evidence.

Write down what happened.

Save what you can.

Ask for help early.


© 2026 Click Giraffe