Hackers Against Humans

A party game for people who click things.

3 or more players. No security knowledge needed. Every fake email is built from four parts. Two are dealt to the table, two come out of your hand.

BEFORE YOU START

Print all 13 card sheets, cut along the guides, and sort into four piles by the coloured band.

- **24 Prompts** — the pretext
- **20 Asks** — what they want
- **32 Senders** — who it's from
- **28 Hooks** — the pressure

SET UP

Put the **Prompt** and **Ask** decks face down in the middle. Shuffle the **Sender** and **Hook** cards together and deal seven to each player. Pick a first **Inbox**. They judge, and do not play.

A ROUND

The Inbox turns over a **Prompt**. Everyone plays a **Sender** and a **Hook** face down, before they know how the email ends. The Inbox turns over an **Ask**, then reads each finished email out loud.

TWO WINNERS EACH ROUND

Catch of the Day, the one most likely to work on a real person, takes the Prompt card. **The Red Herring**, the funniest, takes the Ask card. A card you win is a fish.

Read out the security tip on the winning cards. Learning to spot these is the reason the game exists.

Draw back up to seven. The player to the left becomes the next Inbox. First to seven fish wins.

FIRST-TIMER VERSION

Turn the Ask over first, so players can build towards it.

IF YOU GET A STUCK HAND

Seven cards from one shuffled pile very occasionally come out all Senders or all Hooks, and you can't finish an email with those. Show your hand, put it back and draw seven more. It happens about once in eighty-five deals.

> **Why this works.** Every card in the game is a real technique that gets used on real people. Building the attacks yourself is a faster way to learn the shape of them than being told to watch out. The tell is usually the mismatch: a sender who would never make that ask.

Free to print and play inside your organisation. Made by StrongestLayer for Cyber Security Awareness Month.

PROMPT T01

THE URGENT BOSS FAVOR

Subject: **Quick favor**

Hi, it's ___who___ . ___hook___ . Can you ___ask___ ? I'm tied up and can't talk right now.

TIP Urgency plus a boss's authority is textbook business email compromise. Verify odd requests by phone.

PROMPT T02

THE AUTOMATED NOTICE

Subject: **Action required**

This is an automated message from ___who___ . ___hook___ . To continue, ___ask___ .

TIP 'Automated' framing makes fakes feel official. The system look is trivial to copy.

PROMPT T03

THE SECURITY ALERT

Subject: **Security notice**

___who___ security here. ___hook___ . To secure your account, ___ask___ .

TIP Attackers pose as security to rush you. Real teams don't demand action in seconds.

PROMPT T04

THE ACCOUNT NOTICE

Subject: **About your account**

Notice from ___who___ . ___hook___ . To sort this out, ___ask___ .

TIP A vague 'about your account' hook fits any scam. The ask is what reveals the trap.

PROMPT T05

THE FRIENDLY HEADS-UP

Subject: **Heads up**

Hey, it's ___who___ . ___hook___ , so ___ask___ when you get a sec. Thanks!

TIP A casual, friendly tone lowers your guard as much as a formal one. Verify anyway.

PROMPT T06

THE IT TICKET

Subject: **Ticket #48213**

___who___ from support. ___hook___ . To restore full access, ___ask___ .

TIP Fake IT tickets feel routine. Real support never needs your password.

PROMPT T07

THE DELIVERY NOTICE

Subject: **Delivery update**

___who___ : ___hook___ . To fix this, ___ask___ .

TIP Delivery notices are among the most-clicked scams. Track only on the official app.

PROMPT T08

THE BILLING NOTICE

Subject: **Billing**

___who___ , accounts team. ___hook___ . To avoid a fee, ___ask___ .

TIP A looming fee manufactures urgency. Check any bill through the real account, not the email.

PROMPT T09

THE FORMAL REQUEST

Subject: **Time-sensitive request**

Dear colleague, this is _who_. _hook_. Please _ask_ at your earliest convenience.

TIP Formal, polished language is not proof. Style is the easiest thing to fake.

PROMPT T10

THE REPLY THREAD

Subject: **Re: as discussed**

Following up, _who_ here. _hook_. As agreed, _ask_.

TIP A fake 'Re:' implies a history that never happened, so the request feels pre-approved.

PROMPT T11

THE OFFICIAL NOTICE

Subject: **Official notice**

This is _who_. _hook_. To resolve this, _ask_ within 24 hours.

TIP A 24-hour clock is pressure, not procedure. Real notices give you time and options.

PROMPT T12

THE HR NOTICE

Subject: **Please review**

From _who_. _hook_. To keep things current, _ask_ by end of day.

TIP HR-themed phish spikes at review and enrollment time. Use the official portal, not the link.

PROMPT T13

THE ACCOUNT ALERT

Subject: **Alert**

who alert: _hook_. To protect your account, _ask_.

TIP 'Protect your account' is the bait that leads to a fake login. Go to the real site yourself.

PROMPT T14

THE RECEIPT

Subject: **Your receipt**

Thanks from _who_. _hook_. If this wasn't you, _ask_.

TIP Fake receipts bait you to 'cancel' via a scam link or number. Ignore the contact details given.

PROMPT T15

THE OPPORTUNITY

Subject: **For you**

Hi! _who_ here. _hook_. To move ahead, _ask_.

TIP Too-good opportunities harvest data or fees. Verify the source and never pay to take part.

PROMPT T16

THE REWARD

Subject: **You're selected**

Good news from _who_! _hook_. To claim it, _ask_.

TIP 'You've been selected' for something you didn't enter is a lure. Prizes never need a password.

PROMPT T17

THE APPEAL

Subject: **A quick ask**

who reaching out. hook . Would you ask today?

TIP Urgent appeals exploit goodwill. Act through an official site you found yourself, not a link.

PROMPT T18

THE LEGAL NOTICE

Subject: **Notice**

This is who . hook . To avoid further action, ask .

TIP Legal-threat scare tactics rush you to pay. Real action doesn't arrive as a surprise email.

PROMPT T19

THE MAILBOX NOTICE

Subject: **Mailbox**

Automated notice from who . hook . To keep your mail, ask .

TIP 'Mailbox full, act now' is a credential trap. Manage storage from your real mail settings.

PROMPT T20

THE CALENDAR INVITE

Subject: **Invite**

who invited you. hook . To confirm, ask .

TIP Malicious invites hide phishing links. Don't click links inside unexpected meeting invites.

PROMPT T21

THE DOCUMENT SHARE

Subject: **Shared with you**

who shared a file. hook . To open it, ask .

TIP Fake 'shared file' notices lead to credential traps. Open documents from the source, not the email.

PROMPT T22

THE SETUP STEP

Subject: **Finish setup**

who needs one step. hook . ask to finish.

TIP A single 'quick step' is how many attacks get their foothold. Verify before you complete it.

PROMPT T23

THE CONFIDENTIAL NOTE

Subject: **Between us**

who here. hook . Keep this quiet, but ask .

TIP Secrecy plus a special request is textbook fraud. Confidentiality is a manipulation tactic.

PROMPT T24

THE VERIFICATION

Subject: **Verify**

who needs to verify it's you. hook . To confirm, ask .

TIP 'Verify it's you' is how credential and code theft starts. Confirm on the real site, never a link.

THE ASK

confirm your login on this page

TIP Lookalike login pages steal passwords. Check the address bar before typing.

THE ASK

reset your password here

TIP Never reset via an email link. Type the site address yourself.

THE ASK

verify your account details

TIP 'Verify your details' pages harvest data. Go to the real site instead.

THE ASK

share the code we just texted you

TIP Never share a one-time code. Real support will never ask for it.

THE ASK

approve the login request on your phone

TIP Approving a prompt you didn't start hands over your account. Deny unexpected ones.

THE ASK

approve this wire transfer

TIP Verify every wire by calling a known number. Wires are hard to reverse.

THE ASK

pay this invoice to the new account

TIP 'New bank details' on an invoice is a classic redirect scam. Confirm with the vendor.

THE ASK

buy 5 gift cards and send the codes

TIP Gift cards are the top scam payment. No real boss or agency is paid this way.

THE ASK

update your direct-deposit details

TIP Payroll changes are a favorite fraud. Confirm in person or by phone.

THE ASK

pay the redelivery fee

TIP Real carriers don't collect fees by text or email link. Track on the official app.

THE ASK

track your package here

TIP Fake tracking links harvest logins and cards. Use the carrier's own app.

THE ASK

send me the W-2s

TIP Payroll and W-2 data requests are a known scam. Verify before sending anything.

THE ASK

reply with the staff contact list

TIP Attackers harvest directories for the next attack. Confirm before sharing.

THE ASK

open the attached file

TIP Unexpected attachments carry malware. Confirm with the sender first.

THE ASK

install this security app

TIP Unexpected 'required' installs can be malware. Verify with IT.

THE ASK

scan this QR code

TIP QR codes hide their real destination (quishing). Don't scan codes from emails.

THE ASK

call this number right away

TIP Attacker-supplied numbers lead to fake support. Use official contacts only.

WHO IT'S FROM

The CEO

TIP CEO impersonation drives billions in fraud. Real chiefs don't demand secrecy or gift cards.

THE ASK

reply to confirm you received this

TIP Even a reply confirms your address is active. Be cautious with unknown senders.

WHO IT'S FROM

The CFO

TIP Finance leaders are top impersonation targets. Confirm money requests on a known number.

THE ASK

view the message in your browser

TIP 'View in browser' links can lead anywhere. Hover and check before clicking.

WHO IT'S FROM

Your manager

TIP Display names are trivial to fake. An out-of-character request deserves a real check.

THE ASK

update your email signature

TIP Odd 'update your signature' steps can plant malicious links. Verify with IT.

WHO IT'S FROM

The IT help desk

TIP Real IT never needs your password to help you.

WHO IT'S FROM

HR

TIP Fake HR spikes at review and enrollment time. Use the official portal, not the link.

WHO IT'S FROM

The security team

TIP Attackers pose as security to rush you. Real teams don't demand action in seconds.

WHO IT'S FROM

The payroll team

TIP Direct-deposit change requests are a top fraud. Confirm in person.

WHO IT'S FROM

The finance team

TIP Payment requests by email should always be verified another way.

WHO IT'S FROM

A coworker

TIP Compromised colleague accounts send real-looking phish. An odd tone is a red flag.

WHO IT'S FROM

The front desk

TIP A familiar internal sender can still be spoofed. Verify unusual asks.

WHO IT'S FROM

Your bank

TIP Banks never ask you to confirm full credentials by email.

WHO IT'S FROM

The tax office

TIP Tax agencies mail first and never demand instant payment.

WHO IT'S FROM

Microsoft

TIP Brand names are easy to fake. Check the real address, not the logo.

WHO IT'S FROM

Google

TIP A real Google alert links to google.com, not a lookalike. Check the address bar.

WHO IT'S FROM

DocuSign

TIP Fake e-sign emails harvest logins. Go to the service directly.

WHO IT'S FROM

A delivery company

TIP Redelivery-fee messages are a classic scam. Track only on the official app.

WHO IT'S FROM

Amazon

TIP Order and refund scams impersonate Amazon. Check orders in the app, not the email.

WHO IT'S FROM

Your phone carrier

TIP Carrier alerts that ask for codes or logins are usually fake.

WHO IT'S FROM

LinkedIn

TIP Fake connection and job messages harvest data. Verify on the site itself.

WHO IT'S FROM

The building landlord

TIP Payment-detail updates are often scams. Confirm through a trusted channel.

WHO IT'S FROM

Your doctor's office

TIP Health portals get phished too. Log in directly, never via the email.

WHO IT'S FROM

LeBron James

TIP If the sender makes no sense for the ask, that mismatch is the whole tell. Stop and verify.

WHO IT'S FROM

Your grandma

TIP Attackers impersonate people you love to lower your guard. Verify unusual asks with a real call.

WHO IT'S FROM

A Roman emperor

TIP Authority is a trick, not proof. A grand title in an email means nothing on its own.

WHO IT'S FROM

Dracula

TIP Phish often need you after hours when help is scarce. Off-hours pressure is a warning sign.

WHO IT'S FROM

A pirate captain

TIP Hand over your treasure is every scam in a nutshell: a stranger wants your money.

WHO IT'S FROM

Santa Claus

TIP 'You've been chosen' generosity is a lure. Unexpected gifts usually cost you something.

WHO IT'S FROM

Bigfoot

TIP If you can't verify who is really behind it, treat the request as unproven.

WHO IT'S FROM

The office plant

TIP When the sender is absurd, the spell breaks. Notice that same mismatch on real emails.

THE HOOK

This is time-sensitive and confidential.

TIP Secrecy plus speed is the signature of fraud. That combo should raise alarms.

WHO IT'S FROM

Biscuit the golden retriever

TIP Cute or familiar framing can't verify identity. Check the actual address.

THE HOOK

Please handle this before end of day.

TIP Deadlines manufacture pressure. Real requests can wait for a quick check.

WHO IT'S FROM

A soap-opera villain

TIP Drama and urgency are bait. Calm, boring verification beats them every time.

THE HOOK

I'm going into a meeting and can't call.

TIP 'Can't talk right now' blocks the easiest check: a phone call. Call anyway.

WHO IT'S FROM

A medieval knight

TIP Grand claims and pressure are manipulation. Slow down before you act.

THE HOOK

This needs to happen today.

TIP Urgency is the most common manipulation lever. Slow down.

THE HOOK

Sorry for the short notice.

TIP Short notice is engineered, not accidental. Don't let it rush you.

THE HOOK

Keep this between us for now.

TIP Requests for secrecy exist to stop you verifying. That is the red flag.

THE HOOK

It will only take a minute.

TIP 'Quick and easy' lowers your guard. The ask still deserves scrutiny.

THE HOOK

I'd appreciate a fast turnaround.

TIP Politeness plus pressure is still pressure. Verify before acting.

THE HOOK

Please don't let this slip.

TIP Guilt and urgency are levers. A real colleague will understand a quick check.

THE HOOK

Your account has been locked.

TIP Lockout threats push you to a fake login. Go to the real site yourself.

THE HOOK

We detected a suspicious login.

TIP Don't click the 'secure it' link. Open the site directly and check.

THE HOOK

Your password expires today.

TIP Password-reset bait harvests credentials. Reset only from the real site.

THE HOOK

There's a problem with your last payment.

TIP Fake billing problems push you to a lookalike page.

THE HOOK

You have an unpaid invoice.

TIP Unexpected invoices are a top malware and fraud trick. Confirm with the vendor.

THE HOOK

Your package couldn't be delivered.

TIP Missed-delivery notices are among the most-clicked scams. Use the official app.

THE HOOK

You have a new voicemail.

TIP Voicemail-by-email links often lead to fake logins. Check your phone system.

THE HOOK

Your storage is almost full.

TIP 'Full mailbox, verify now' is a credential trap. Manage storage in real settings.

THE HOOK

A document is waiting for your signature.

TIP 'Review and sign' is a common login trap. Open the service directly.

THE HOOK

Your benefits are about to lapse.

TIP Benefits scares spike at enrollment. Use the official HR portal.

THE HOOK

A goose has entered the building.

TIP Chaos and urgency are bait. The calmer you stay, the safer you are.

THE HOOK

Mercury is in retrograde and so is your account.

TIP When the reason makes no sense, that's your cue to stop and verify.

THE HOOK

The office coffee machine has gained sentience.

TIP Any 'act now' story, however absurd, is designed to skip your judgment.

THE HOOK

The Wi-Fi says it misses you.

TIP Emotional hooks lower your guard. Notice when a message tugs at feelings.

THE HOOK

Your free trial of oxygen is ending.

TIP 'Your X is ending' is a template. Verify before you click.

THE HOOK

We are critically low on staplers.

TIP Fake internal crises get you to act fast. Confirm through normal channels.

THE HOOK

Your horoscope demands immediate action.

TIP No real request depends on acting 'immediately'. Urgency itself is the flag.

THE HOOK

The printer has unionized.

TIP A weird pretext is a reason to doubt, not to click.

THE HOOK

The break-room fridge has been breached.

TIP 'Breach, act now' is exactly how real scare-phish reads. Pause and confirm.