

The Mac Phishing Playbook: How Attacks on Mac Teams Work in 2026, and What Your Staff Should Do Next

A practical guide for business owners and IT leads at UK Mac-first businesses who need to brief their team on the phishing attacks reaching Macs right now.

Last updated: October 2026

Included in this PDF:

- The Mac Phishing Playbook
- Checklist: What Leadership Should Put in Place This Month
- Staff card: Spot It, Report It

Other relevant resources:

- [A Guide to Building a Stronger Security Culture](#)
- [macOS 27 Is Live: The Security Changes That Will Quietly Break on Your Mac Fleet](#)

Phishing aimed at Mac users has changed shape this year. The attacks we're warning clients about now arrive as calendar invites, fake "fix your Mac" pages and convincing copies of Apple's own launch pages, and the most effective ones get a member of staff to run the attacker's code for them. Apple has added protections along the way, and attackers have already found routes around some of them. This guide explains what these attacks look like, what your staff should do when something seems off, and what leadership should put in place this month.

PART 1

Why are attackers now targeting Mac users?

Macs now sit on the desks of exactly the people attackers want to reach: founders, finance teams, creative leads and account managers in agencies and professional services firms. Those people hold the logins to email, client files, banking portals and the cloud tools the business runs on. The Mac is simply how attackers get to them.

Is a Mac safer than a PC against phishing?

A Mac does a lot to stop software it doesn't trust. Gatekeeper checks where an app came from, and XProtect blocks known malware before it runs. Phishing doesn't need to beat any of that. It persuades a person to type their password into a fake page, or to run a command they've been told will fix a problem. Once the user has done the work themselves, the Mac's defences have very little to object to.

So the honest answer is that a Mac makes life hard for malware, and phishing goes around it by targeting the person at the keyboard. A team that believes "we're on Macs, so we're safe" is easier to fool, because it isn't looking.

What are attackers actually after?

Access, mostly. The malware behind the Mac campaigns in this guide, with Atomic Stealer the most common, is built to collect browser logins, saved passwords, Keychain data, crypto wallets and files. A stolen login is often worth far more than the Mac it came from. With it, an attacker can read email, reach shared drives and sign in to your cloud services, and nobody may notice for days.

PART 2

What do phishing attacks on Mac teams look like in 2026?

Very few of them look like the badly spelt email from a foreign prince that staff were trained to spot. These are the five patterns we'd want every Mac team to recognise.

Fake meeting invites in your calendar

An invite appears in Calendar for a "document review", a "contract signature" or an HR meeting, with a link to join or view. Many calendar apps add invites automatically, before anyone accepts them, and the event can stay on the calendar after the original email has been deleted. The link usually leads to a fake sign-in page. Accepting or declining the invite also tells the sender the address is live.

"Fix your Mac" pages (ClickFix)

A web page claims something is wrong: the disk is full, the browser is out of date, or you need to prove you're human. It then gives step-by-step instructions to fix it, often styled to look like Apple's own support pages. Following the steps runs the attacker's code. This technique, known as ClickFix, is now one of the main ways malware reaches Macs, and Part 3 covers it in detail.

Fake macOS password and permission prompts

A window that looks like a macOS dialogue asks for your Mac password, or asks you to click Allow so a document can open. The real macOS asks for your password when you're installing something or changing a setting that you started. A password prompt that appears out of nowhere while you're on a website, or one that says you need to enter your password to keep reading, is the warning sign. If in doubt, cancel it and open System Settings yourself.

Scams timed to Apple launches

Big Apple launches bring fake offers with them. Ahead of iPhone Duo preorders opening on 16 October, Malwarebytes researchers found a fake preorder site that copied Apple's design

and offered a \$500 voucher for ordering early. Behind it sat the DarkSword exploit chain, aimed at older iPhones that hadn't been updated. Opening the page on a vulnerable phone was enough to start the attack, with no form to fill in. Launch weeks deserve a short reminder to staff, and they're a good reason to make sure every device is on current software.

Stolen or borrowed logins

In October, ASOS confirmed that an attacker had obtained an employee's login credentials by impersonating a trusted contact, then used them to reach information on third-party platforms the company relied on. Customer names and contact details were among the data accessed. No Mac exploit was involved. The lesson for any business is that the most damaging phishing is usually about a single login, and the people best placed to stop it are staff who feel able to report something odd quickly.

PART 3

What is ClickFix, and why does it matter for Mac teams?

ClickFix is a delivery technique, not a specific piece of malware. Instead of breaking into the Mac, it talks the user into running a command themselves. Because the user starts it, the command runs with their permissions, and the Mac treats it as something they chose to do. 9to5Mac's security coverage now describes ClickFix as the leading way malware is delivered to Macs.

How a ClickFix attack works

1. Someone lands on a web page from a search result, an advert or a link in an email or message.

2. The page says there's a problem with their Mac and offers a quick fix, usually dressed up to look like Apple.
3. The instructions tell them to copy a command and paste it into Terminal, or to click a button that opens a Mac app for them.
4. The command quietly downloads malware, typically Atomic Stealer, which collects passwords and data and sends them to the attacker.

Nothing has been hacked in the traditional sense. The user ran it, and that's what makes it hard for technical controls alone to stop.

What Apple's Terminal warning stops, and what it doesn't

With macOS Tahoe 26.4, Apple added a warning that appears when someone pastes a potentially harmful command into Terminal. It's a genuinely useful change, and it interrupts the classic copy-and-paste version of ClickFix.

Attackers adapted quickly. Jamf Threat Labs found a campaign that skips Terminal altogether. A button on a fake Apple page triggers a link that opens Script Editor, the Mac's built-in scripting app, with the malicious script already loaded and ready to run. Because nothing is pasted into Terminal, the new warning never appears. Script Editor shows its own prompt on recent versions of Tahoe, but if the user clicks through it, the script runs and installs Atomic Stealer.

Apple's warning helps, but it isn't a policy. A prompt that someone can click through only slows an attack down. Your staff need one simple rule that covers every version of this trick: no website ever needs you to open Terminal or Script Editor, and no genuine fix asks you to paste or run anything.

What macOS 27's app and command-line control adds

macOS 27, released in September 2026, lets IT decide through device management which apps and command-line tools are allowed to run on a Mac. Anything not on the approved list is blocked by macOS itself, command-line tools included. For ClickFix, that changes the outcome: even if someone follows the fake instructions, the malware the script tries to run isn't on the list, so it doesn't run.

It needs Macs that are managed through a DMS (formerly MDM) that supports the new controls, and it needs planning. A strict approved list will also block legitimate tools your team relies on, so roll it out to a pilot group first and widen it once the list is right.

PART 4

What should staff do when something looks wrong?

How quickly something is reported shapes how bad it gets. A report within minutes of a click gives IT time to reset a password or isolate a Mac before an attacker uses what they've taken. A report the next morning often doesn't.

Report it, don't forward it

Forwarding a suspicious email to colleagues to ask "is this real?" spreads the link to more people. Use your business's reporting route instead, whether that's a report button in Mail or Outlook, a dedicated address or a message to IT. For a suspicious calendar invite, don't accept, decline or reply. Report it, then delete it once IT has seen it.

What to do if you've clicked a link

- Stop and don't enter anything else on the page.
- Close the page and tell IT straight away, including what you clicked and when.

- If you ran anything, opened Terminal or Script Editor, or downloaded a file, disconnect from Wi-Fi and stop using the Mac until IT tells you otherwise.
- Don't try to clean the Mac up yourself. IT needs to see what happened.

What to do if you've entered your password

- Change the password straight away, from a different device you trust.
- Tell IT, so they can sign you out of every active session and check for anything the attacker changed.
- If you use the same password anywhere else, change it there too.
- If you then get sign-in approval requests you didn't ask for, deny them and report them.

Nobody should get in trouble for reporting. Staff who worry about looking foolish wait, and waiting is what turns a near miss into an incident. Say clearly, and repeat often, that reporting is always the right move, even after a click.

PART 5

What happens after someone reports it?

Staff report more readily when they know what happens next. It's worth sharing a simple version of this with the team.

What IT does in the first hour

1. Speak to the person who reported it and establish what they clicked, typed or ran.

2. If a password was entered, reset it, sign the account out of every session and check that no new sign-in methods or mail forwarding rules have been added.
3. If anything ran on the Mac, isolate it from the network through your device management or security tools.
4. Search for the same message across other mailboxes and remove it, then block the sender, domain or link.
5. Check sign-in logs for access from unusual locations or devices.
6. If others received it, warn the team so nobody else clicks.

When a report becomes an incident

A report becomes an incident once there's evidence the attacker got something: a password that was entered and then used, code that ran on a Mac, or data that was accessed. At that point, follow your incident response plan and keep a written record of what happened and when. If personal data may have been exposed, UK GDPR requires notifiable breaches to be reported to the ICO within 72 hours of the business becoming aware of them, so the clock starts earlier than most people expect.

PART 6

What should leadership put in place this month?

October is Cyber Security Awareness Month, making it a natural time to act. None of the steps below needs a large budget, and most can be done in a week.

1. Choose one reporting route and tell everyone what it is. A single, obvious way to report beats three half-remembered ones.
2. Confirm every Mac, iPhone and iPad is on current software. The iPhone Duo scam worked against devices that had fallen behind on updates.
3. Review how calendar invites are handled. Where your email platform allows it, stop invites from unknown senders being added to calendars automatically.

4. Plan your macOS 27 app and command-line control rollout. Agree a pilot group with IT and start building the approved list.
5. Check MFA on email and your core cloud services. Ask IT whether sign-in can move to phishing-resistant methods such as passkeys.
6. Hand out the staff card. Fill in your reporting route and IT contact, then share it with every member of staff.

If you'd like a second pair of eyes on your reporting process or your macOS 27 rollout plan, **Dr Logic's security team can review both with you** and flag anything that's likely to slow you down when a real report comes in.

Checklist: What Leadership Should Put in Place This Month

A tick-through summary of Part 6 of The Mac Phishing Playbook. Work through it with your IT lead or provider.

Reporting

- ☐ One reporting route agreed

A single button, address or channel that every member of staff knows.

- ☐ No-blame message sent

Staff told in writing that reporting is always right, even after a click.

- ☐ First-hour steps agreed with IT

Everyone knows who resets passwords, isolates Macs and warns the team.

Devices

- ☐ Software updates confirmed

Every Mac, iPhone and iPad checked against current versions in your DMS.

- ☐ macOS 27 app control pilot planned

Pilot group chosen and work started on the approved list of apps and tools.

Accounts

- ☐ MFA checked on core services

Email and key cloud tools confirmed, with passkeys considered where supported.

- ☐ Calendar invite handling reviewed

Automatic adding of invites from unknown senders switched off where possible.

People

- ☐ Staff card filled in and shared

Reporting route and IT contact added, then sent to every member of staff.

- ☐ Launch-week reminder scheduled

A short note to staff ahead of major Apple launches and sales events.

Dr Logic is a UK-based Apple Premium Technical Partner. We help Mac-first organisations stay secure, from device management and security awareness to round-the-clock monitoring. If you'd like help putting the steps in this guide in place, get in touch at drlogic.com.

Dr Logic Ltd. Registered address 26-28 Southernhay East, Exeter EX1 1NS. Registered in England & Wales. Company no. 04947299

Staff Card: Spot It, Report It

Keep this somewhere you'll see it. If something feels off, stop and report it.

SPOT IT

Stop if you see any of these

- A calendar invite you weren't expecting, with a link to view a document or join a meeting.
- A web page saying your Mac has a problem and telling you how to fix it.
- Any instruction to open Terminal or Script Editor, or to paste and run a command.
- A password prompt that appears while you're on a website or reading an email.
- Early access or big discounts on new Apple products, especially before Apple has opened pre orders.
- A message from a "colleague" or "supplier" asking for a login, a change to payment details or something urgent.

REPORT IT

Then do this

1. Don't click, reply or forward it.
2. Report it using the route below.
3. If you clicked or ran something, disconnect from Wi-Fi and call IT straight away.
4. If you typed your password, change it from another trusted device and tell IT.

You will never be in trouble for reporting, even if you've already clicked. The sooner IT knows, the less damage an attacker can do.

Report to:

IT contact and phone: