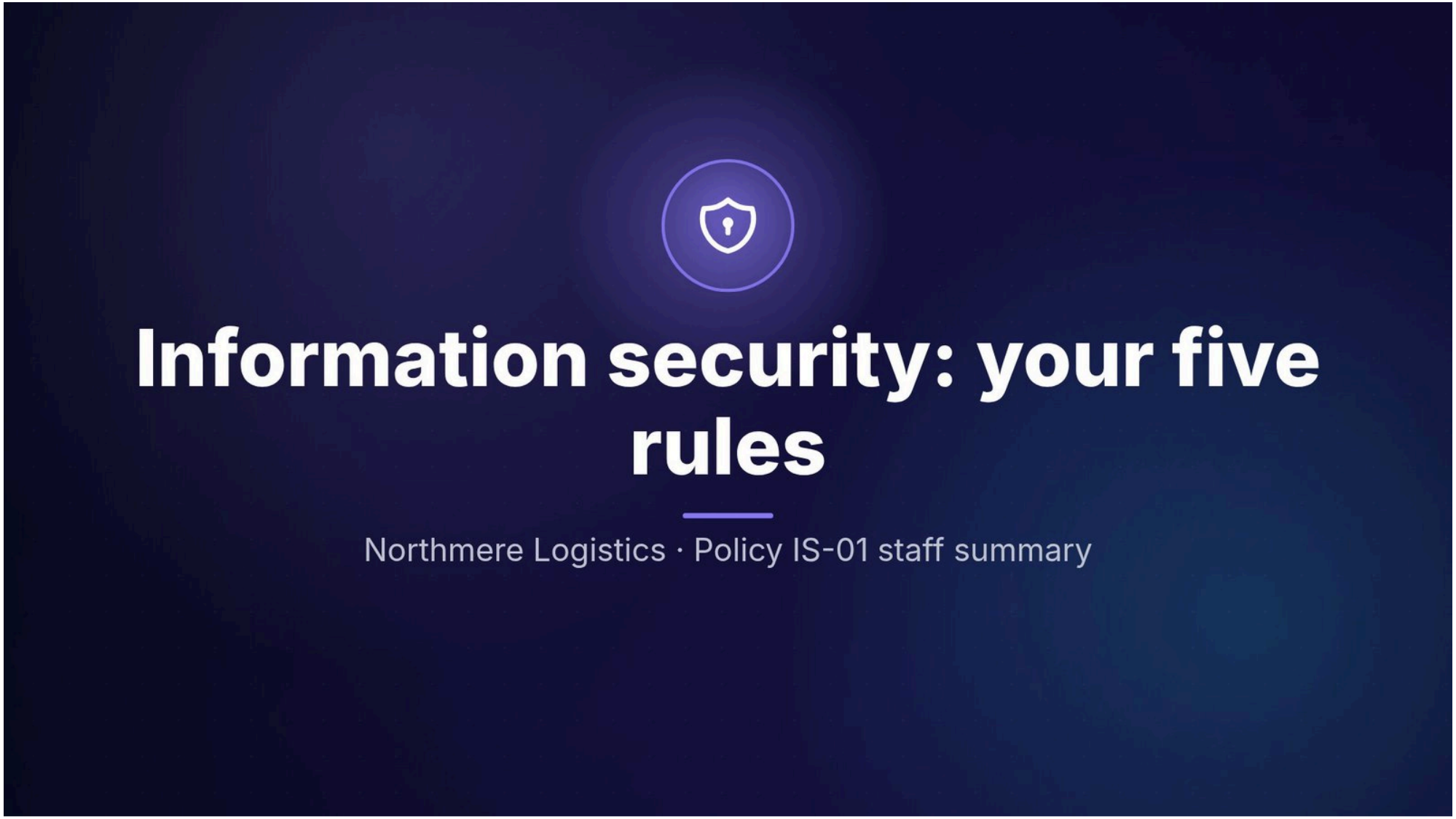
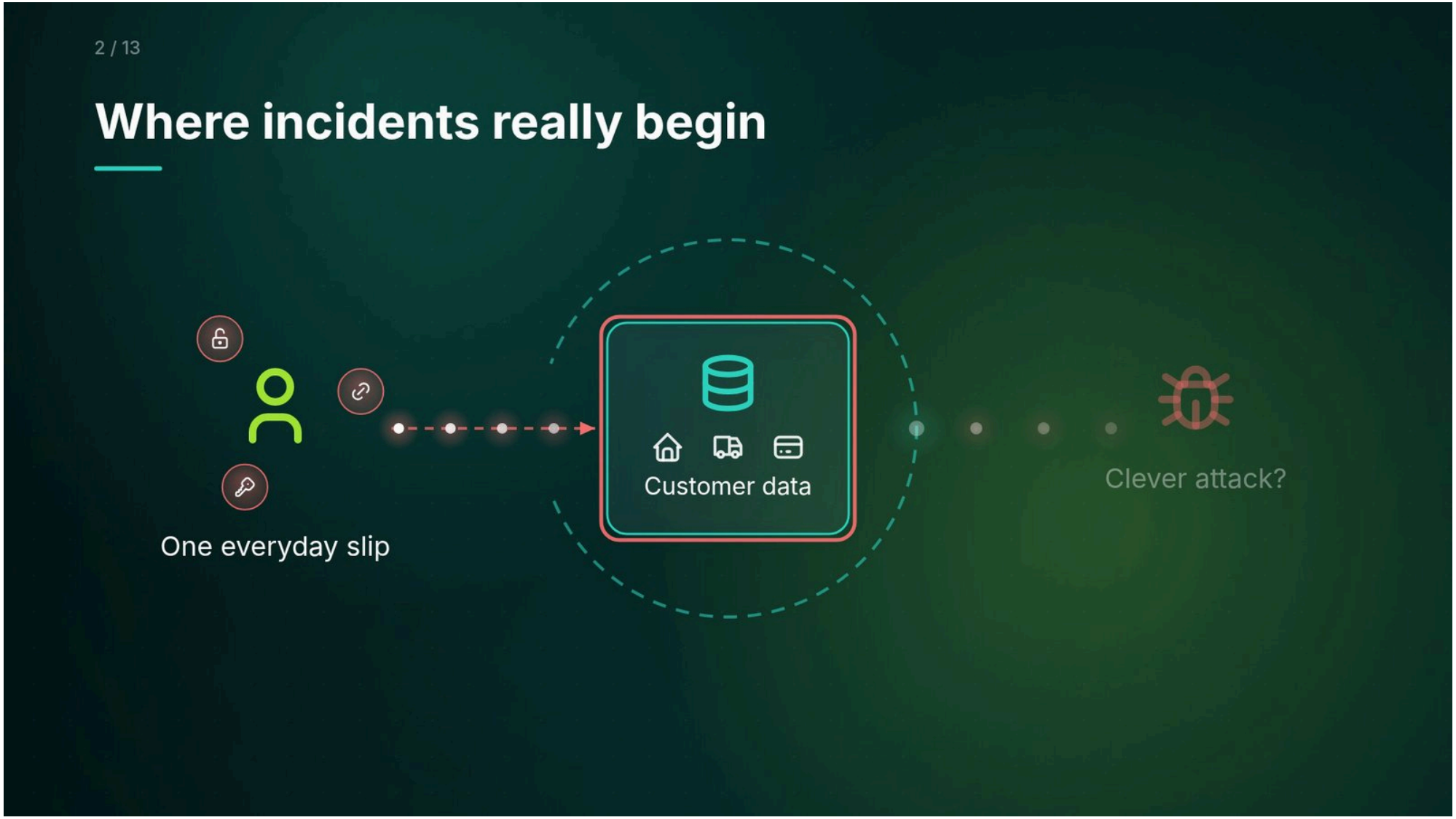


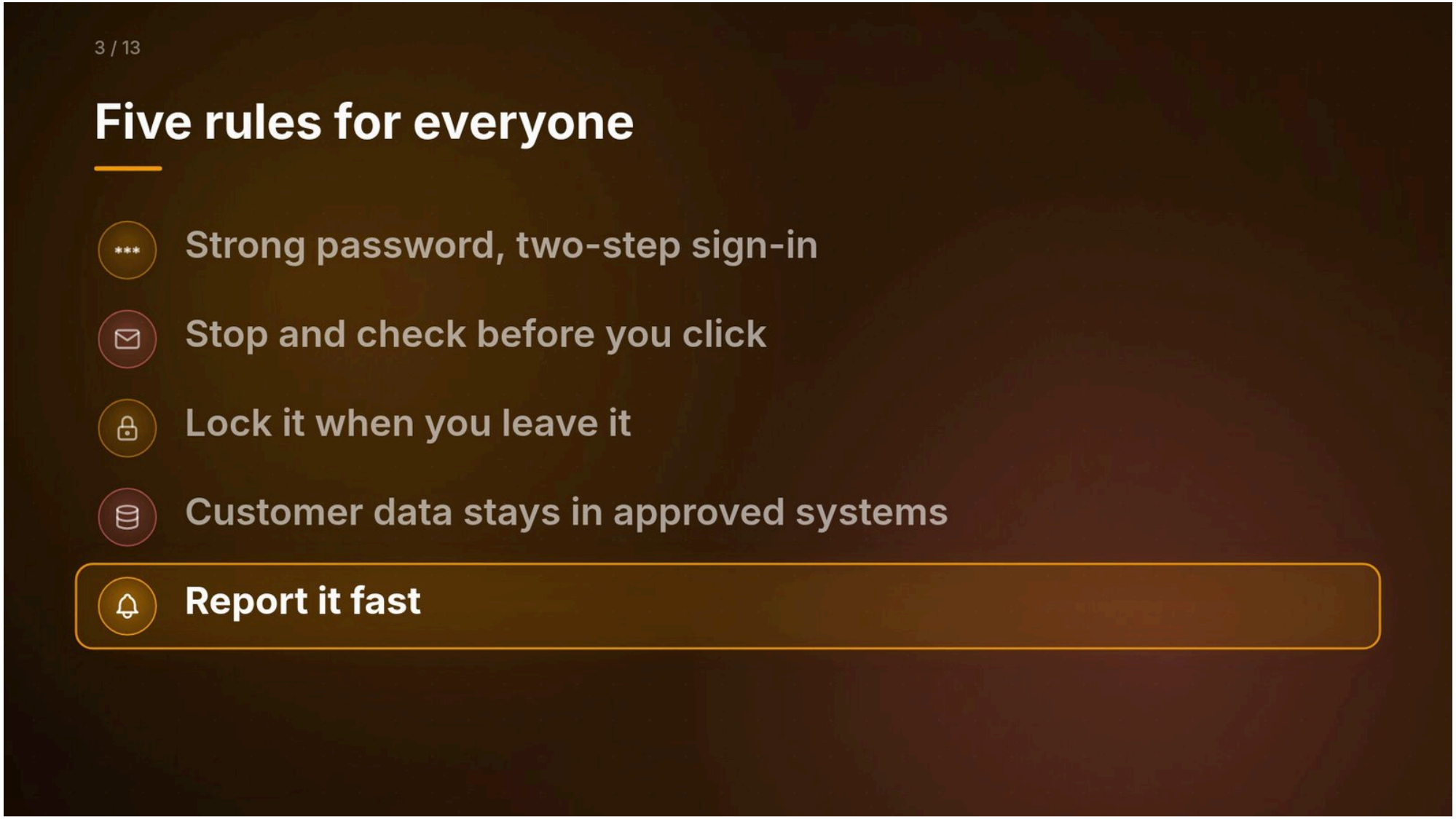
1 / 13 · Security is everyone's job

In the next few minutes, you'll learn the five security rules every Northmere employee and contractor must follow. You'll also learn how to spot a phishing message and exactly what to do when something goes wrong.



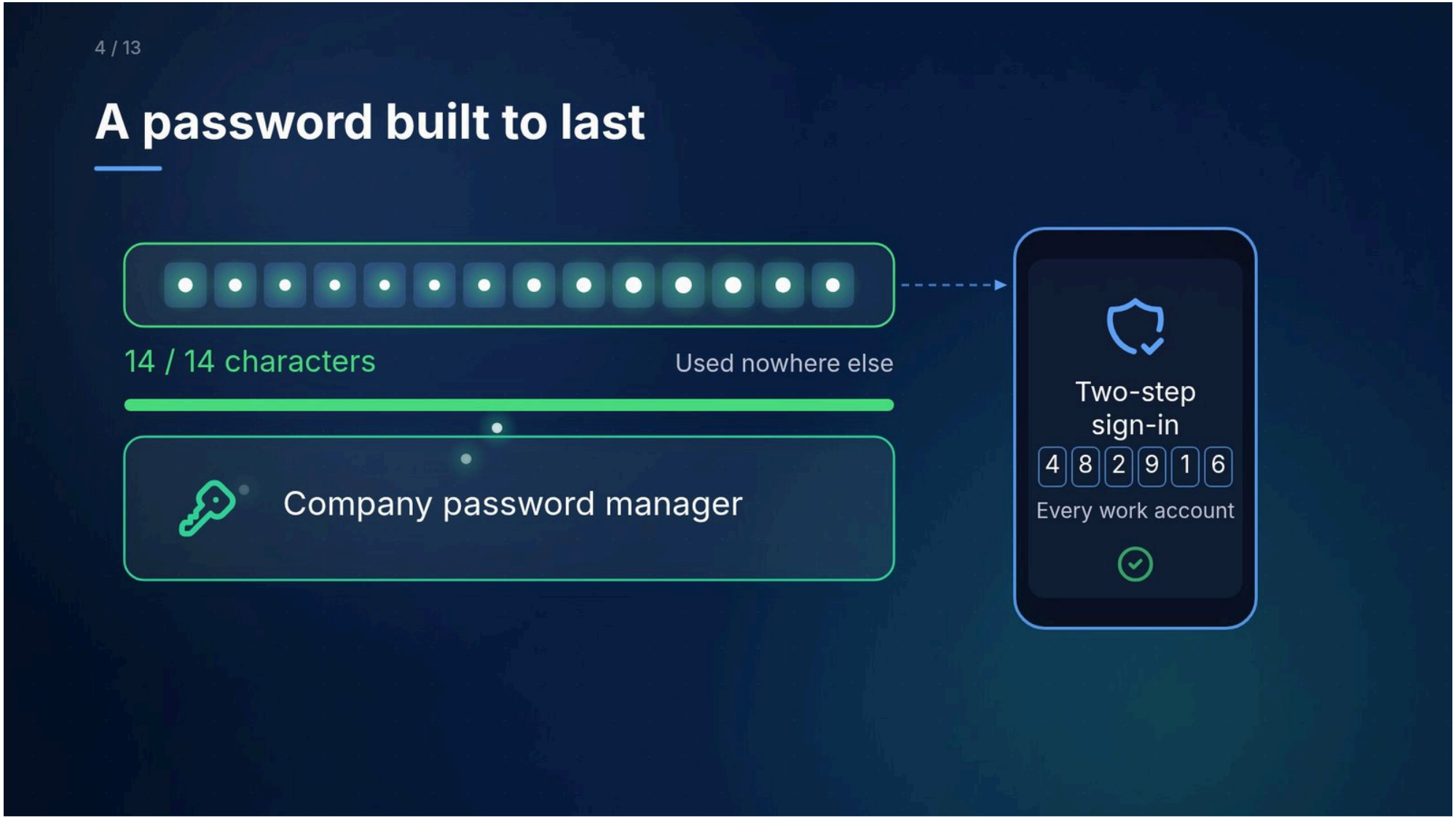
2 / 13 · Why this policy exists

Northmere holds customers' addresses, delivery records and payment details. You might think security incidents start with clever hackers. In fact, most start with one person clicking a link, reusing a password or leaving a laptop unlocked.



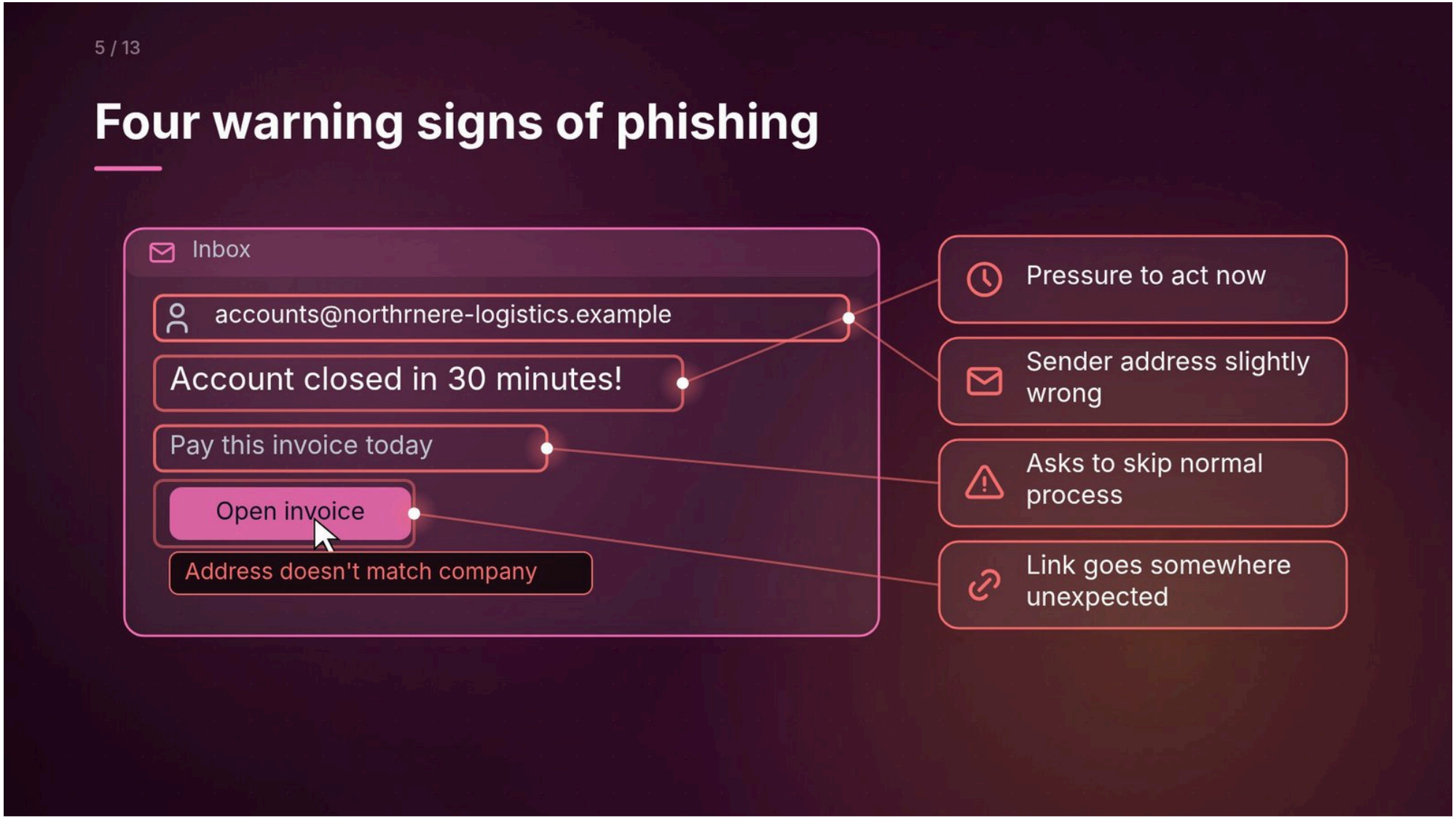
3 / 13 · The five rules

Everything comes down to five rules that apply to everyone. Use a strong password and two-step sign-in. Stop and check before you click. Lock your devices when you leave them. Keep customer data in approved systems, and report problems fast.



4 / 13 · Rule one: passwords

Rule one: your work password must be at least 14 characters long, and used nowhere else. Let the company password manager keep track of it. Two-step sign-in, a second check on top of your password, is required on every work account.



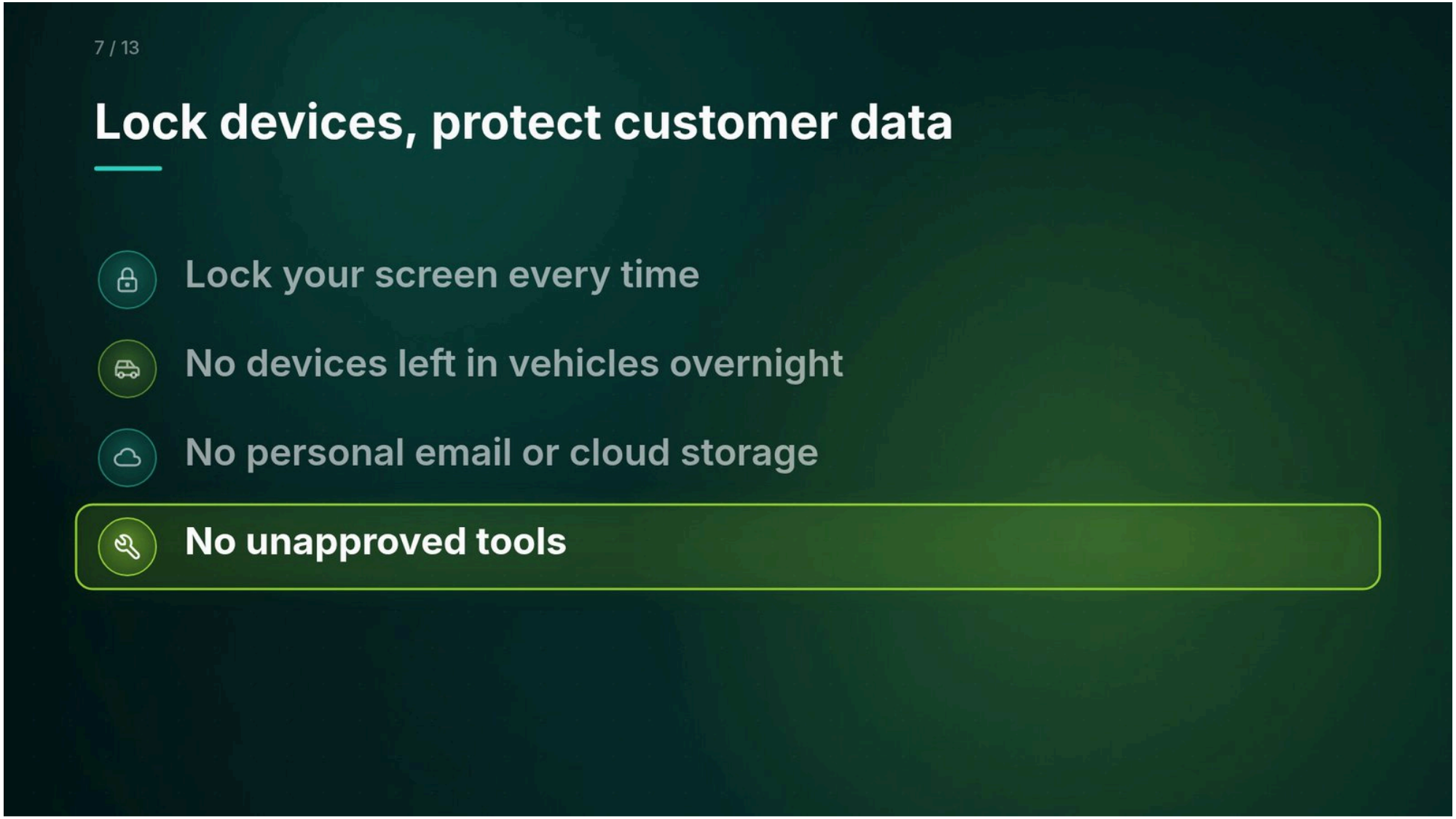
5 / 13 · Spotting phishing

Rule two is about phishing: fake messages designed to trick you. Watch for pressure to act now, like an account closing in 30 minutes. Look for a sender address that's slightly wrong, a request to skip the normal process, or a link that goes somewhere unexpected when you hover over it.



6 / 13 · When you're unsure

If a message makes you unsure, pause. Don't reply and don't click anything. Instead, use the Report phishing button in your email, or forward it to security at northmere dot example.



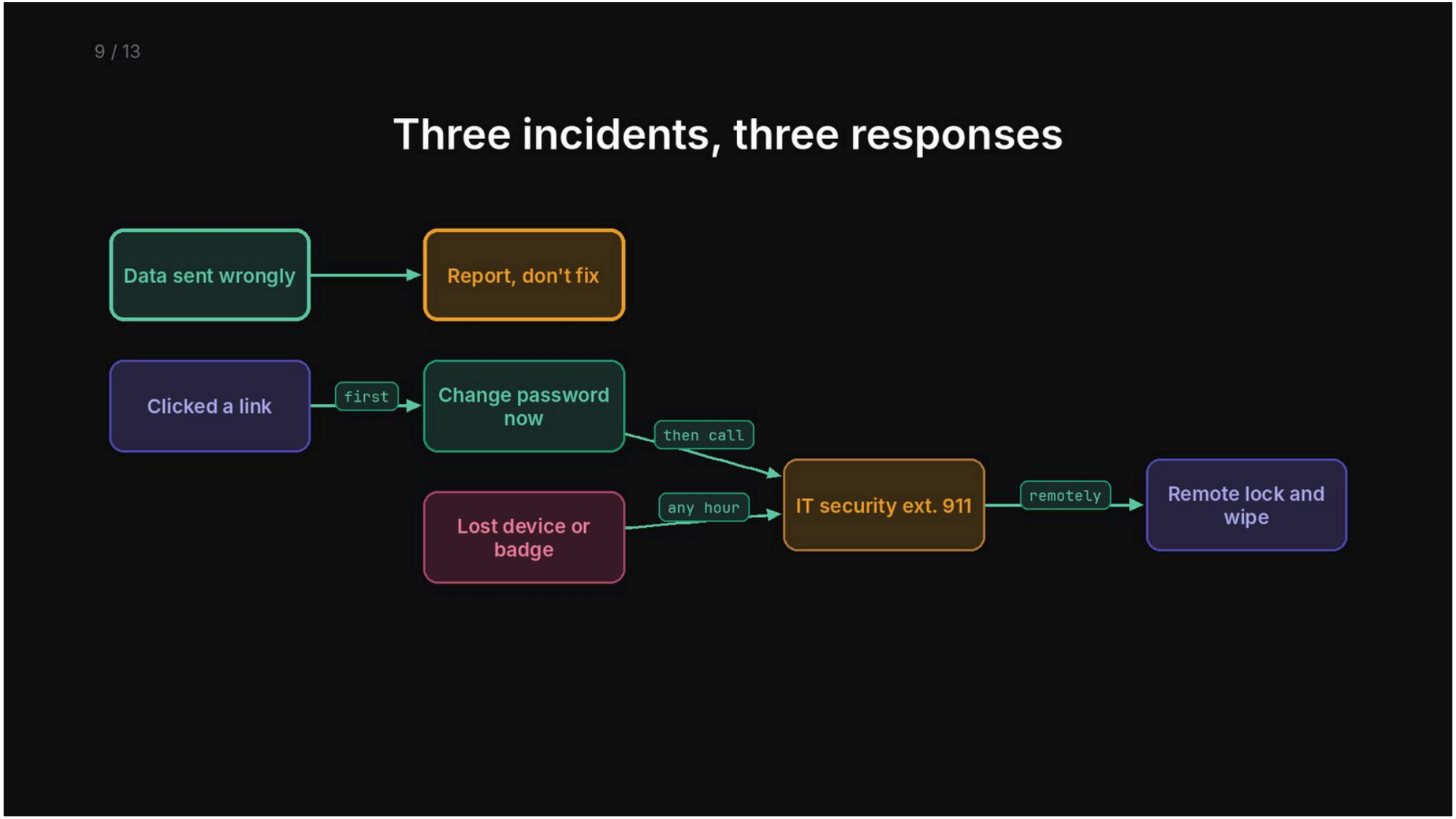
7 / 13 · Rules three and four

Rule three: lock your screen every time you step away, and never leave a laptop or phone in a vehicle overnight. Rule four: keep customer data in approved systems. That means no personal email, no personal cloud storage, and no pasting it into tools the company hasn't approved.



8 / 13 · Rule five: report it fast

Rule five: report it fast. If something looks wrong, report it within one hour, even if you're not sure, and even if it was your mistake. Speed matters, because the company may have to tell the customer and the regulator within 72 hours.



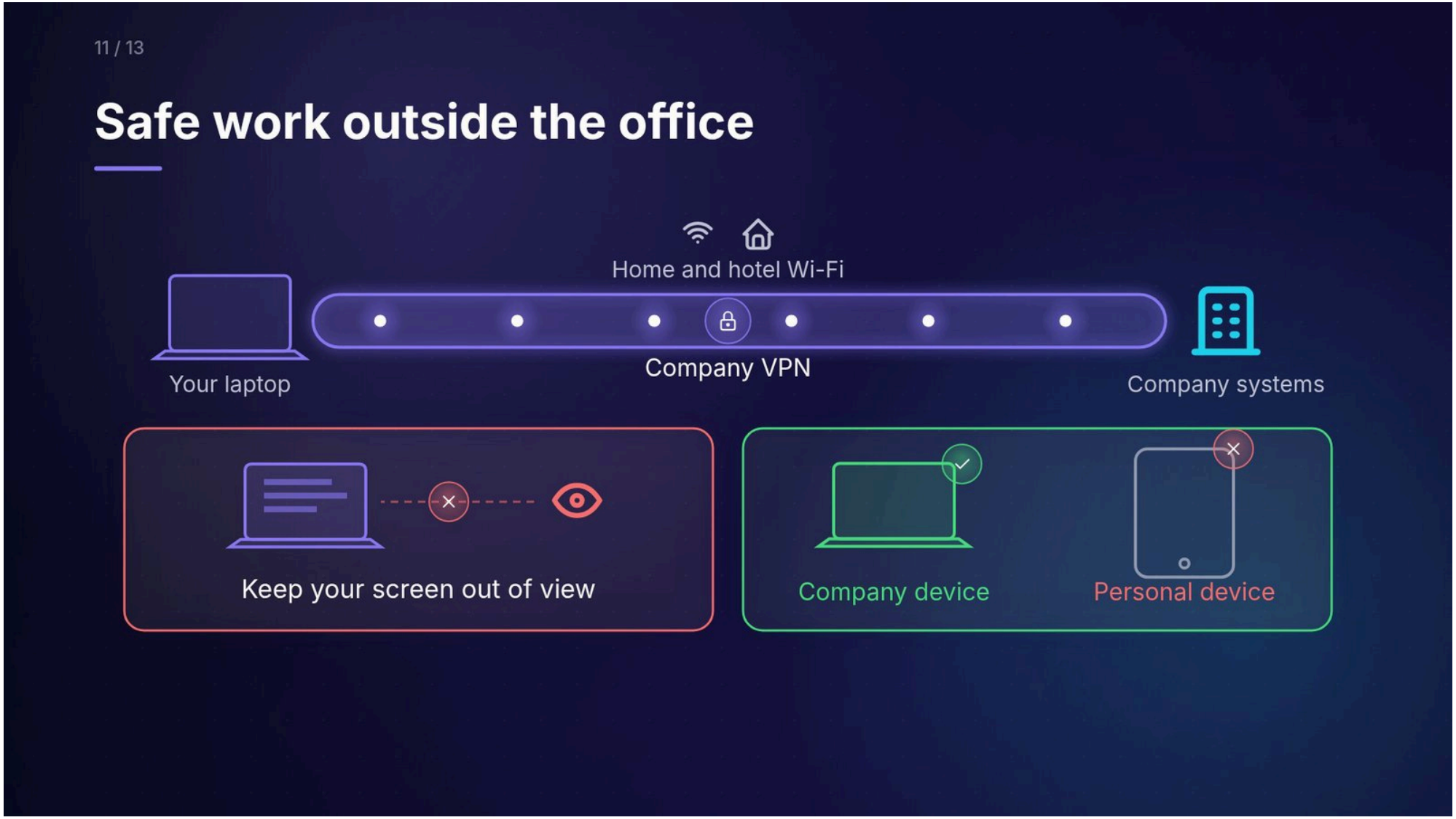
9 / 13 · When something goes wrong

Here's what to do when something goes wrong. Clicked a link or entered your password? Change it straight away, then call the IT security line on extension 911. Lost a laptop, phone or badge? Call that line at once, at any hour, so the device can be locked and wiped remotely. Sent customer data to the wrong person? Don't fix it yourself; report it.



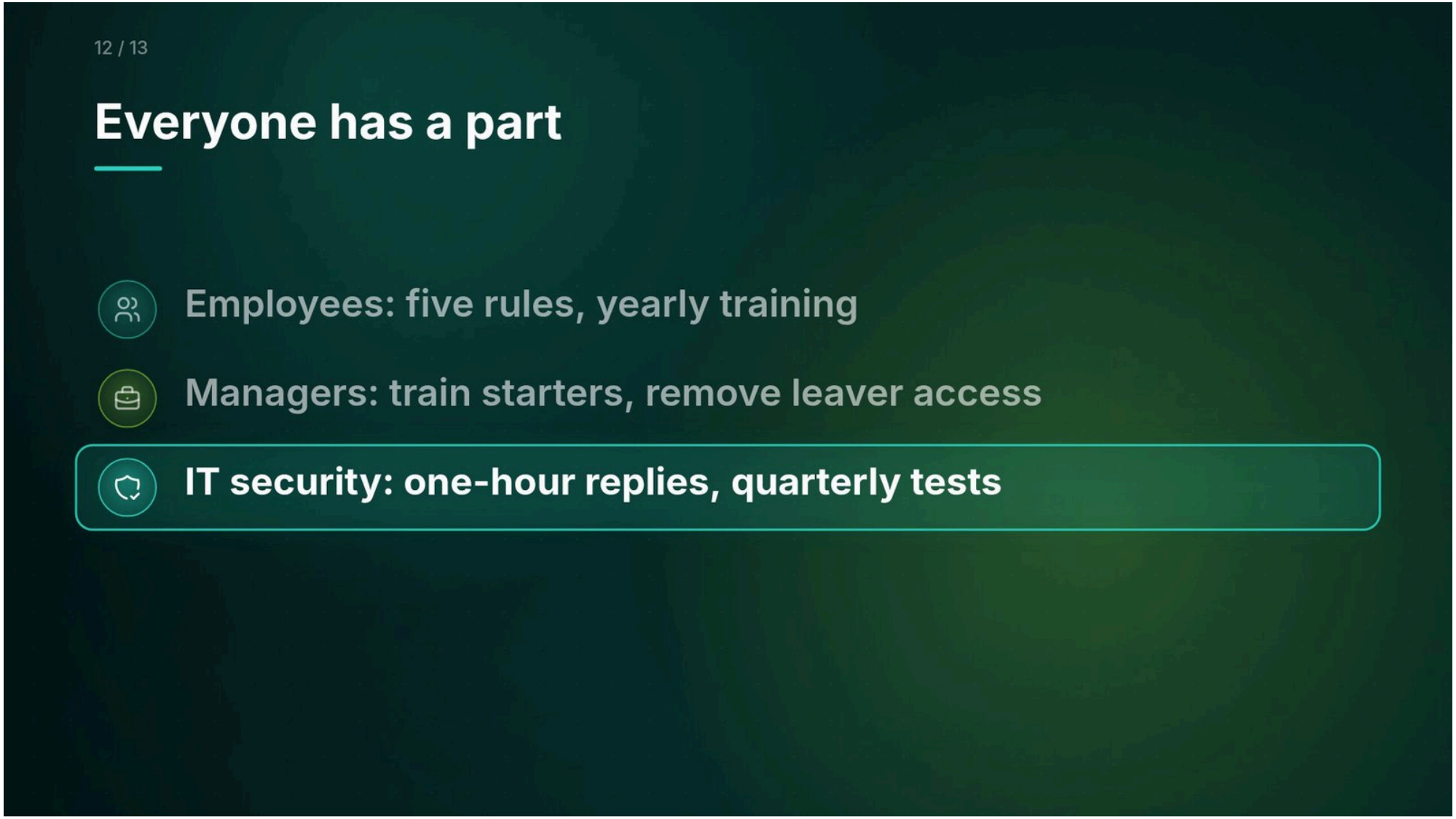
10 / 13 · Report, never hide

You will not be punished for reporting a mistake, but hiding one is a disciplinary matter. And timing changes everything. An incident reported in the first hour is usually contained. One found a week later rarely is.



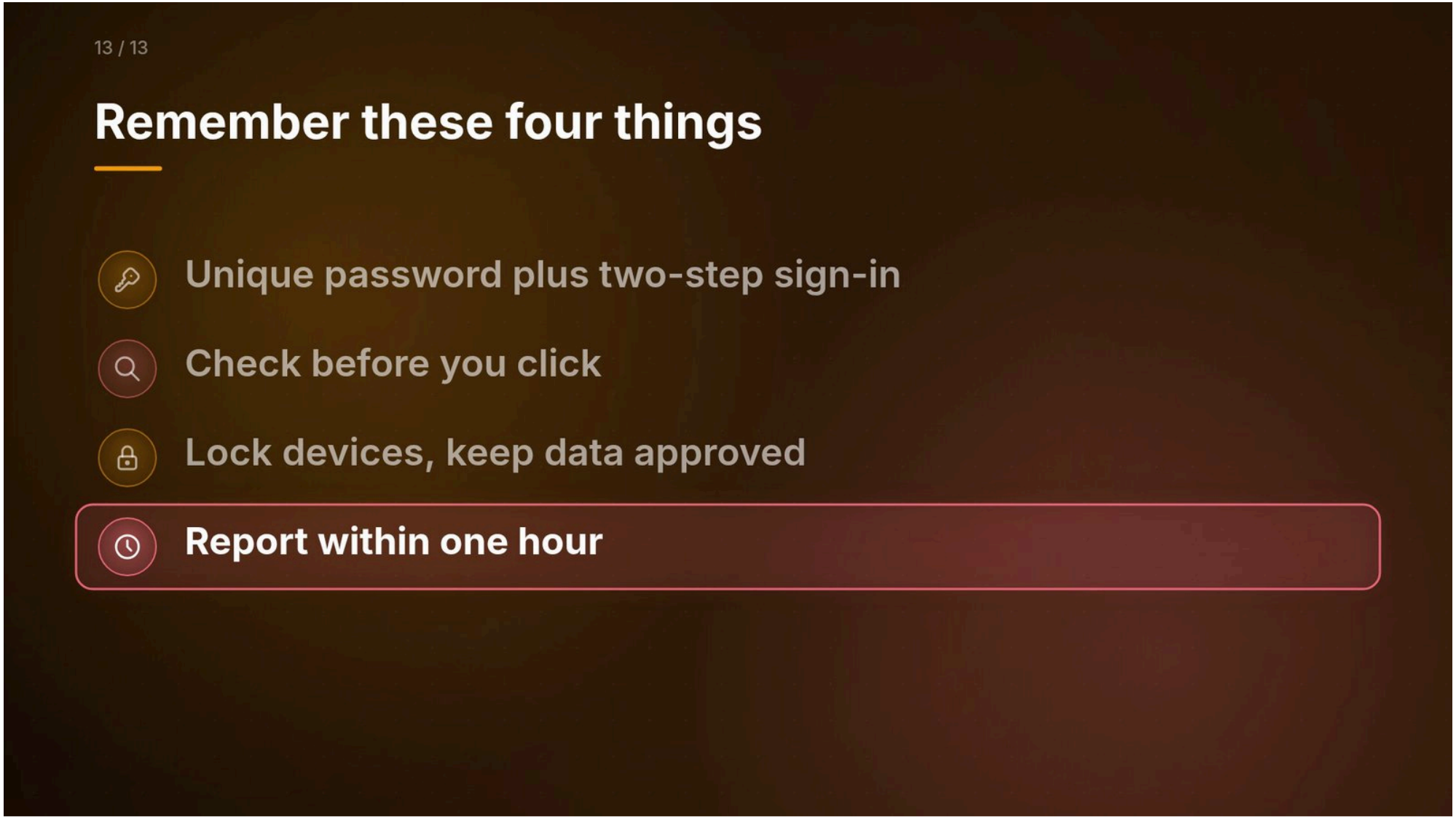
11 / 13 · Working away from the office

Working away from the office? Use the company VPN, a protected connection to company systems, on any network that isn't ours, including home and hotel Wi-Fi. Don't work on customer data where your screen can be seen, such as on a train. And use only company devices; personal laptops and tablets aren't allowed for customer data.



12 / 13 · Who does what

Every employee follows the five rules and completes this training once a year. Managers make sure new starters complete it in their first week, and remove access on a leaver's last day. IT security answers every report within one hour and runs a phishing test each quarter.



13 / 13 · Recap

To recap: use a strong, unique password with two-step sign-in. Stop and check before you click. Lock your devices and keep customer data in approved systems. And if anything looks wrong, report it within the hour. Breaking the policy on purpose or repeatedly can lead to disciplinary action, and the full policy, IS-01, is on the intranet under Policies.