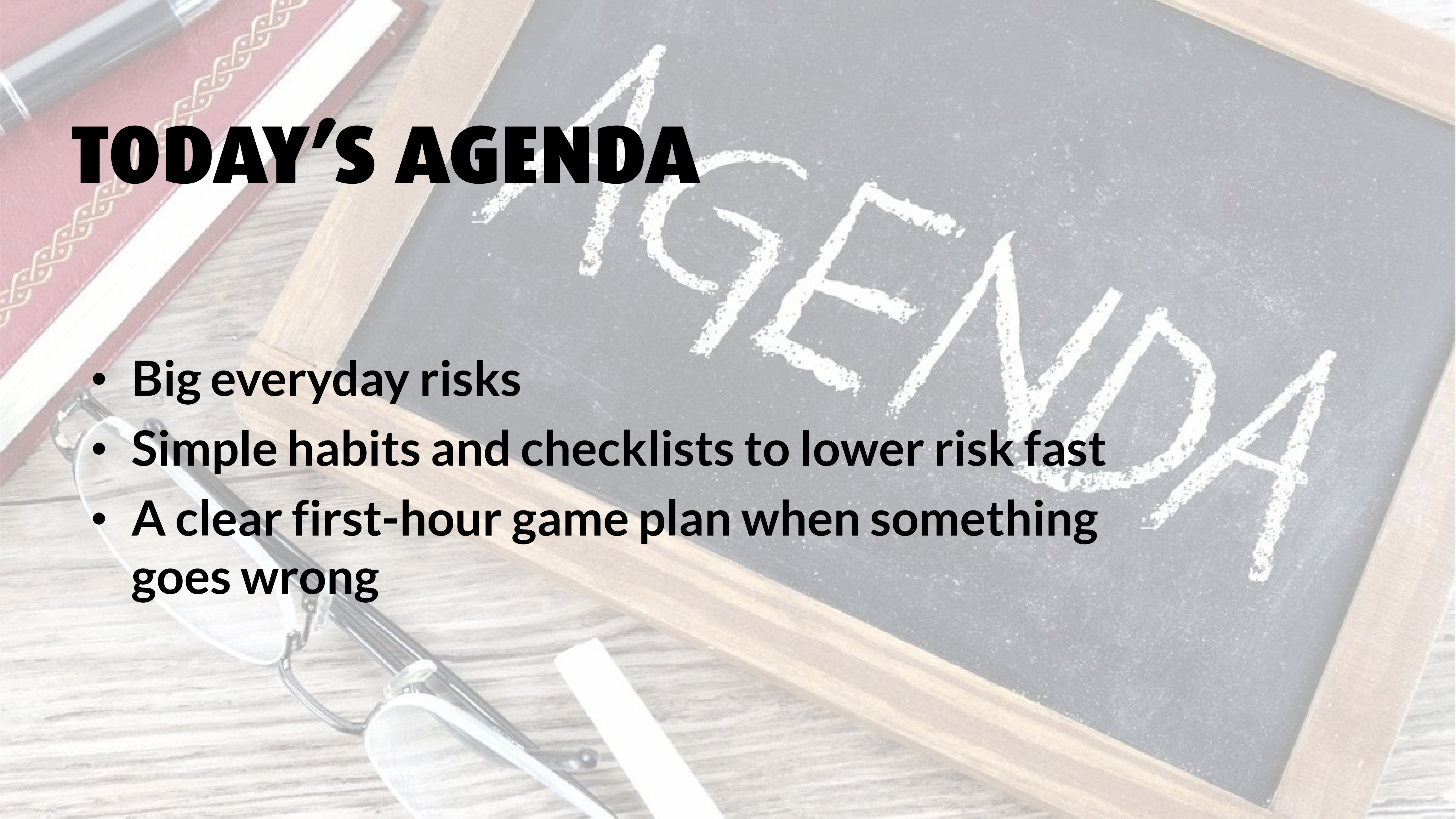
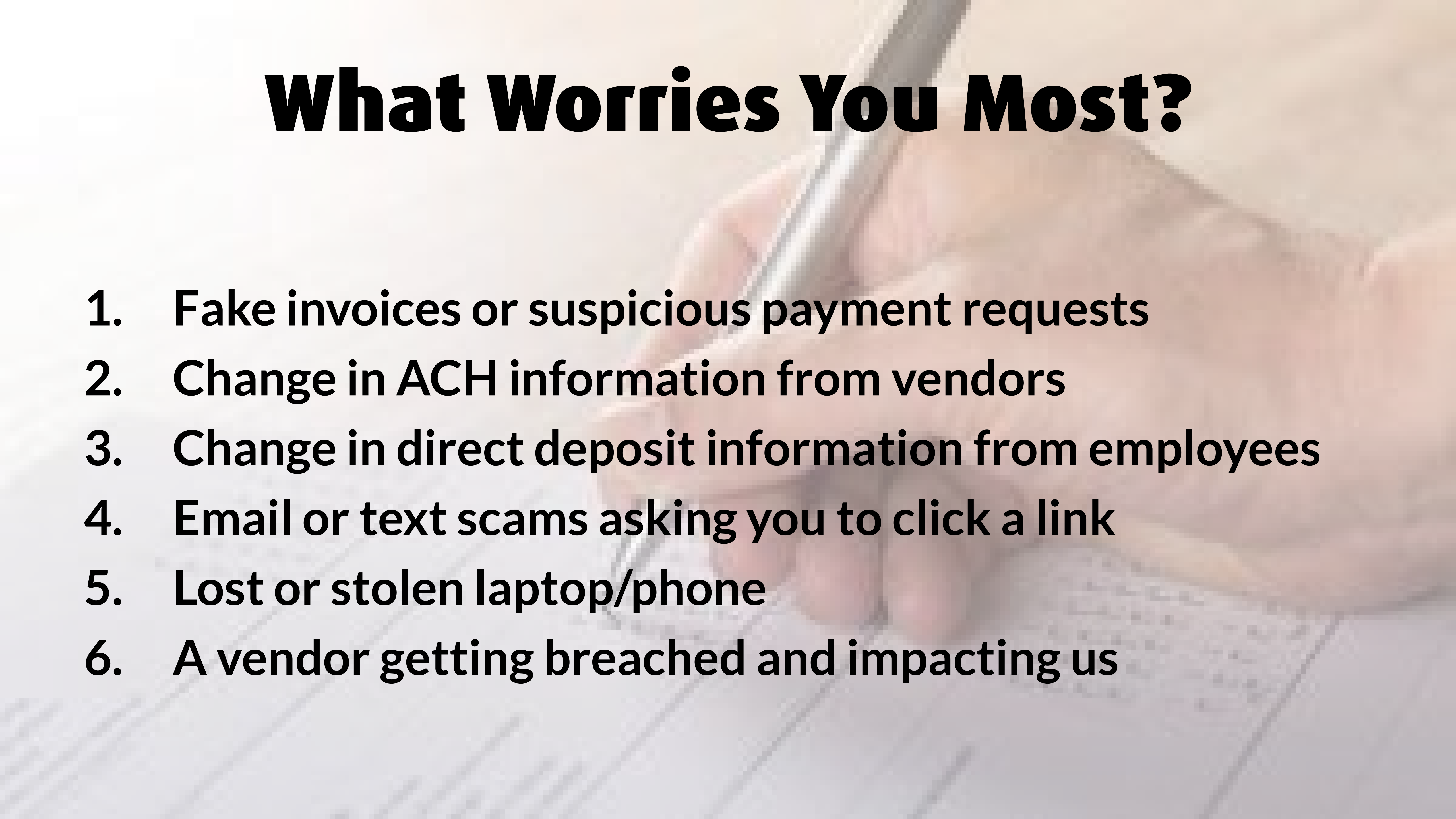
Keeping Your Organization Safe

Assessing & Ensuring Technology Security

TODAY’S AGENDA



- Big everyday risks
- Simple habits and checklists to lower risk fast
- A clear first-hour game plan when something goes wrong



What Worries You Most?

1. Fake invoices or suspicious payment requests
2. Change in ACH information from vendors
3. Change in direct deposit information from employees
4. Email or text scams asking you to click a link
5. Lost or stolen laptop/phone
6. A vendor getting breached and impacting us

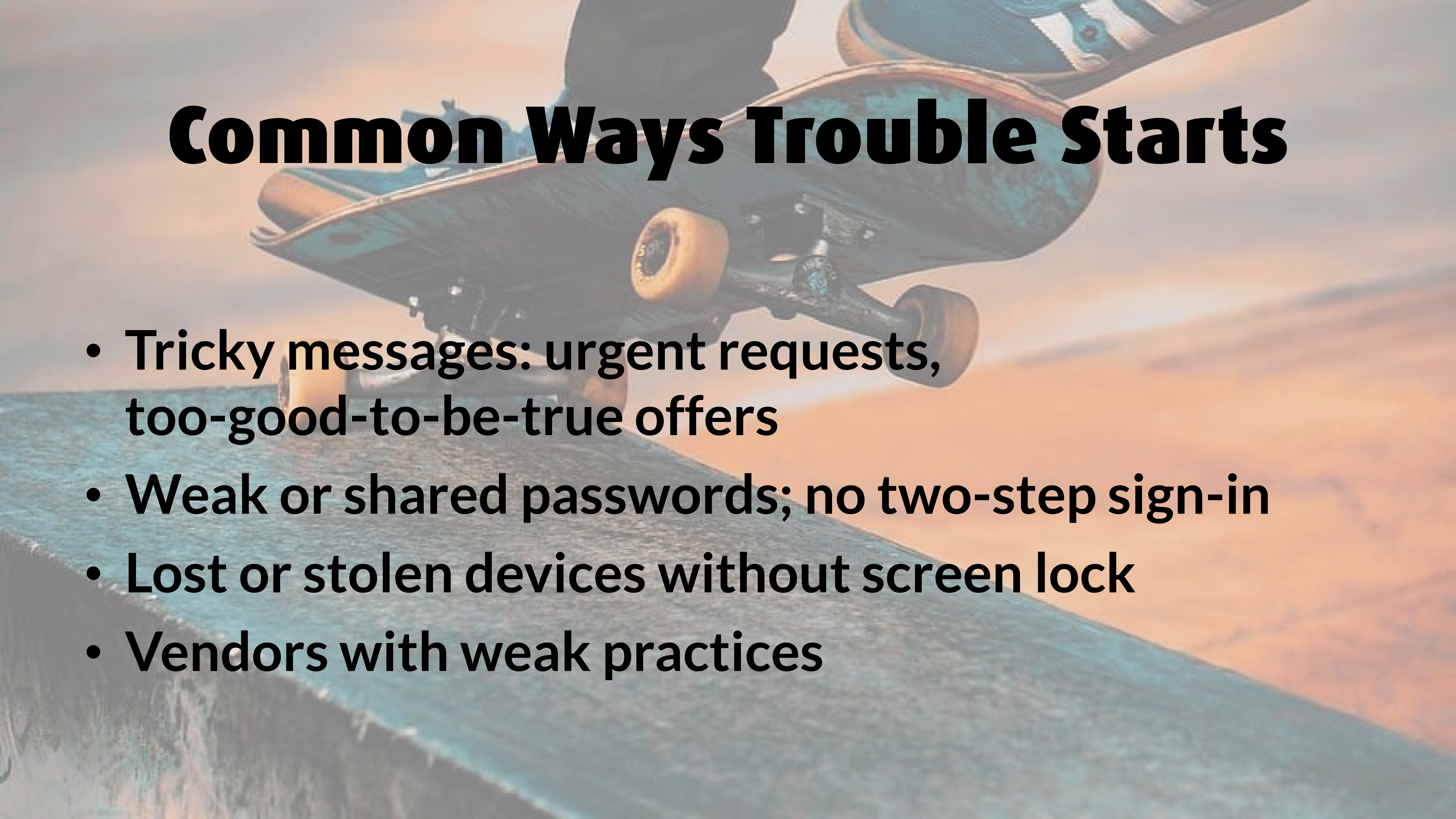
Why This Matters?

- Protecting student and employee information
- Keeping operations running with minimal downtime
- Avoiding costly mistakes and reputational damage
- Meeting policy and legal expectations without the jargon

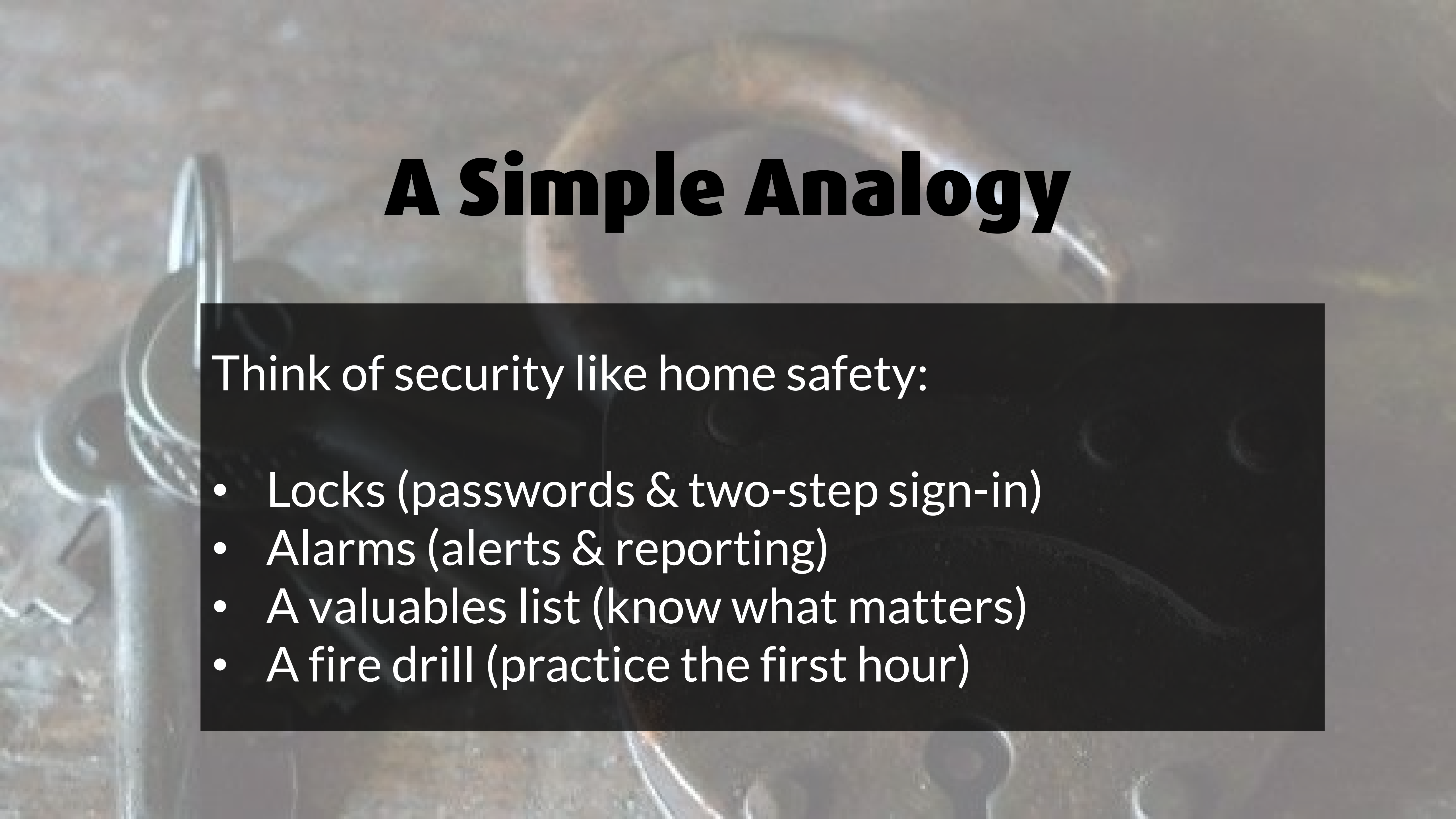
What Are We Protecting?

- People data and payments
- Email and files
- Financial Information and Resources
- Systems and apps we rely on (including cloud/SaaS)

Common Ways Trouble Starts



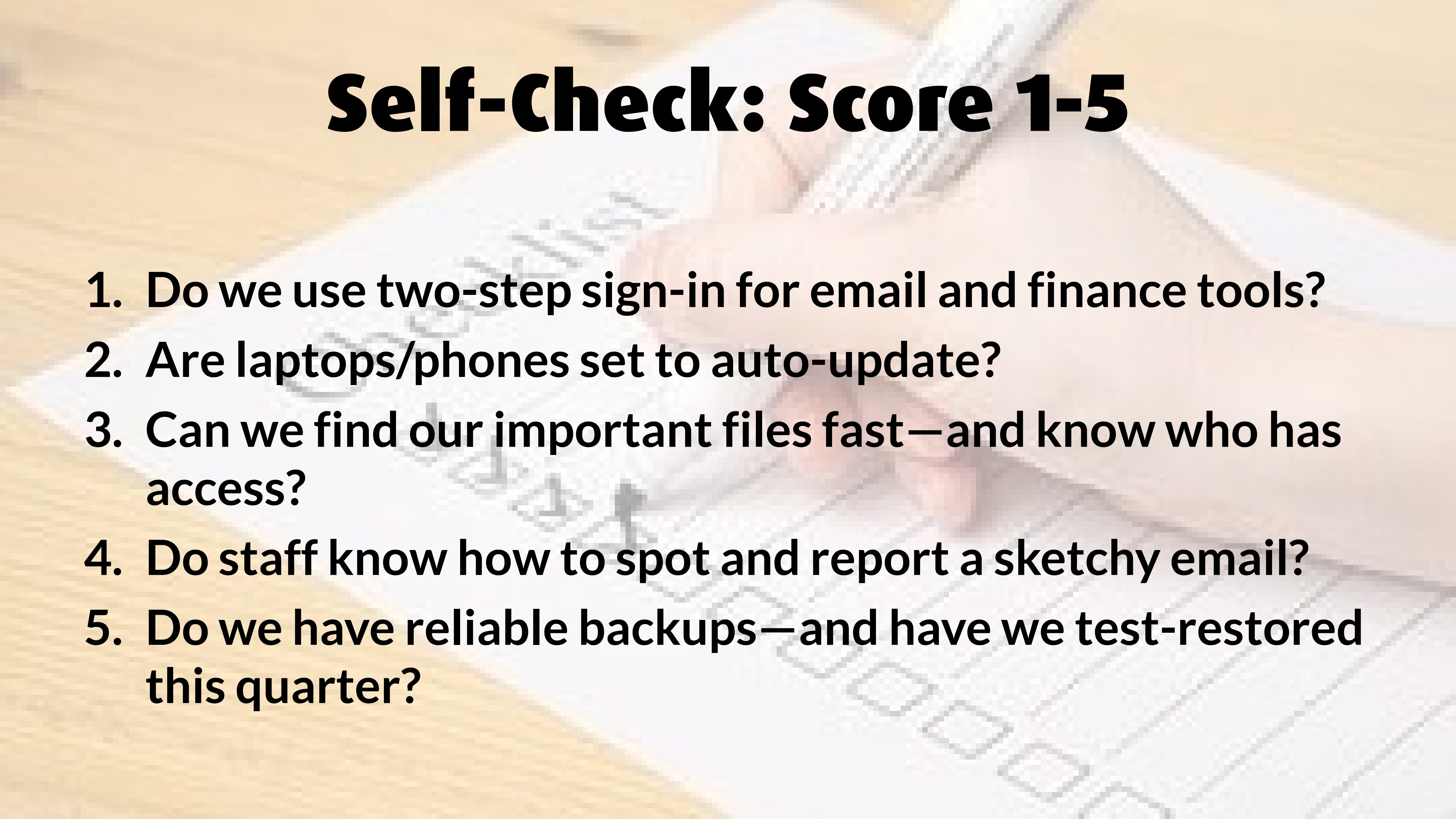
- Tricky messages: urgent requests, too-good-to-be-true offers
- Weak or shared passwords; no two-step sign-in
- Lost or stolen devices without screen lock
- Vendors with weak practices



A Simple Analogy

Think of security like home safety:

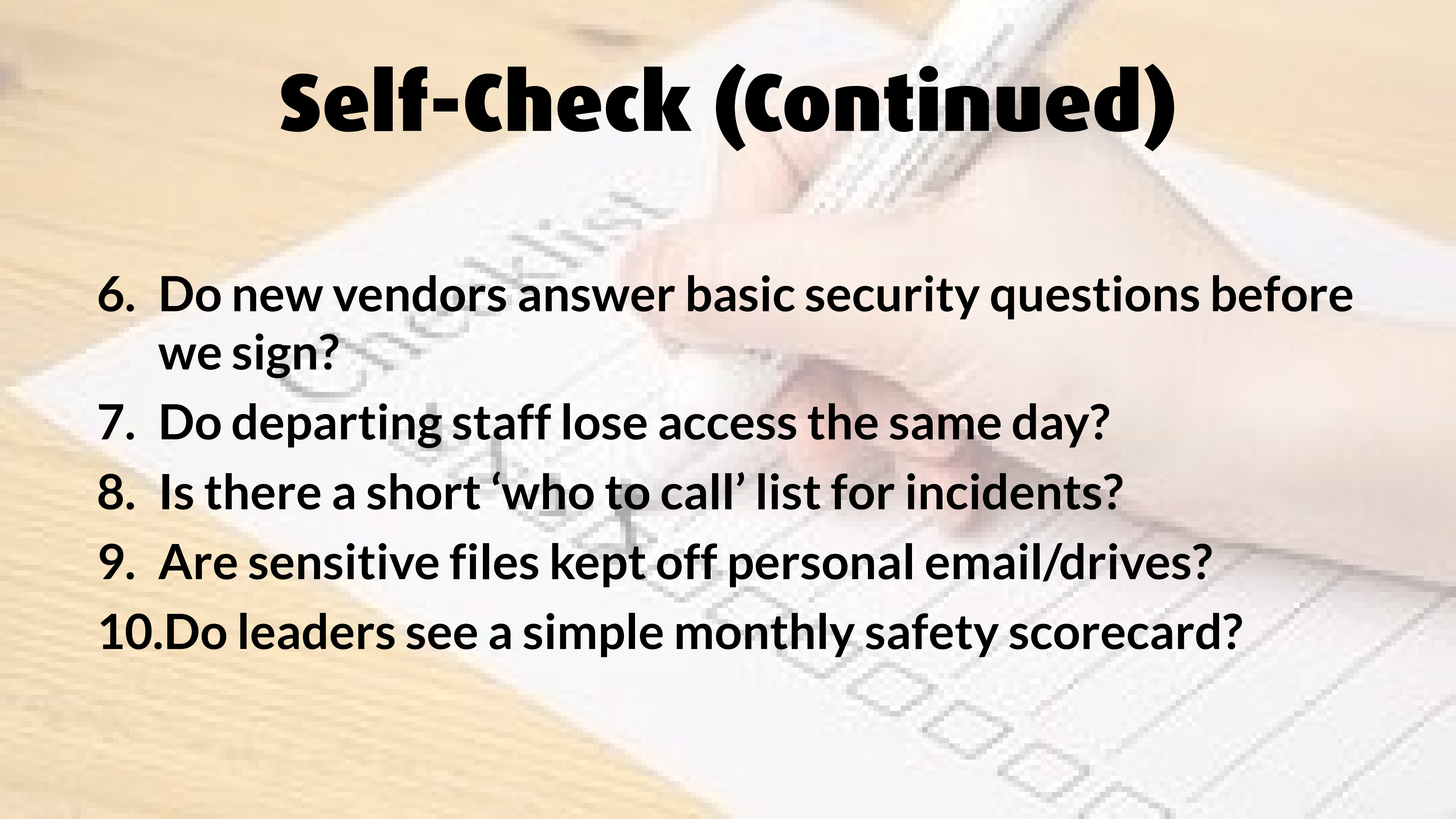
- Locks (passwords & two-step sign-in)
- Alarms (alerts & reporting)
- A valuables list (know what matters)
- A fire drill (practice the first hour)



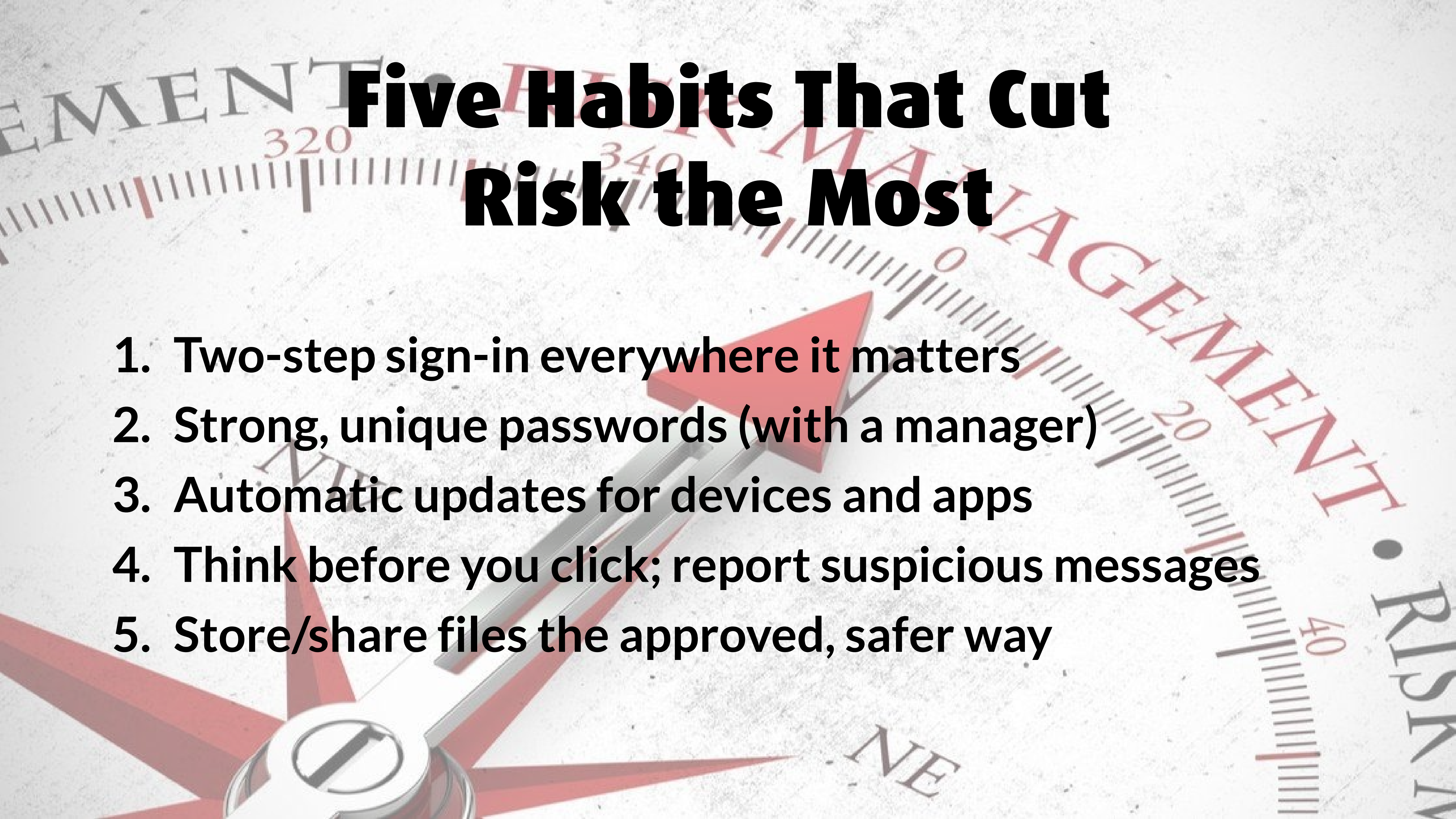
Self-Check: Score 1-5

1. Do we use two-step sign-in for email and finance tools?
2. Are laptops/phones set to auto-update?
3. Can we find our important files fast—and know who has access?
4. Do staff know how to spot and report a sketchy email?
5. Do we have reliable backups—and have we test-restored this quarter?

Self-Check (Continued)



6. Do new vendors answer basic security questions before we sign?
7. Do departing staff lose access the same day?
8. Is there a short ‘who to call’ list for incidents?
9. Are sensitive files kept off personal email/drives?
10. Do leaders see a simple monthly safety scorecard?



Five Habits That Cut Risk the Most

1. Two-step sign-in everywhere it matters
2. Strong, unique passwords (with a manager)
3. Automatic updates for devices and apps
4. Think before you click; report suspicious messages
5. Store/share files the approved, safer way

Habit 1
Two-Step Sign-In

- Add a second check when you sign in (code or app prompt)
- Turn it on for email, HR, payroll, and finance tools first
- Leaders: ask for monthly % of people on 2-step

Habit 2

Strong, Unique Passwords

- Use a password manager (no more sticky notes or reuse)
- Never share passwords; managers can share access safely
- Watch for look-alike login pages; verify the site address

Habit 3

Automatic Updates

- Keep laptops, phones, and key apps on auto-update
- Restart devices regularly so updates can install
- Leaders: ask for % of devices up-to-date each month

Habit 4
Think Before You Click

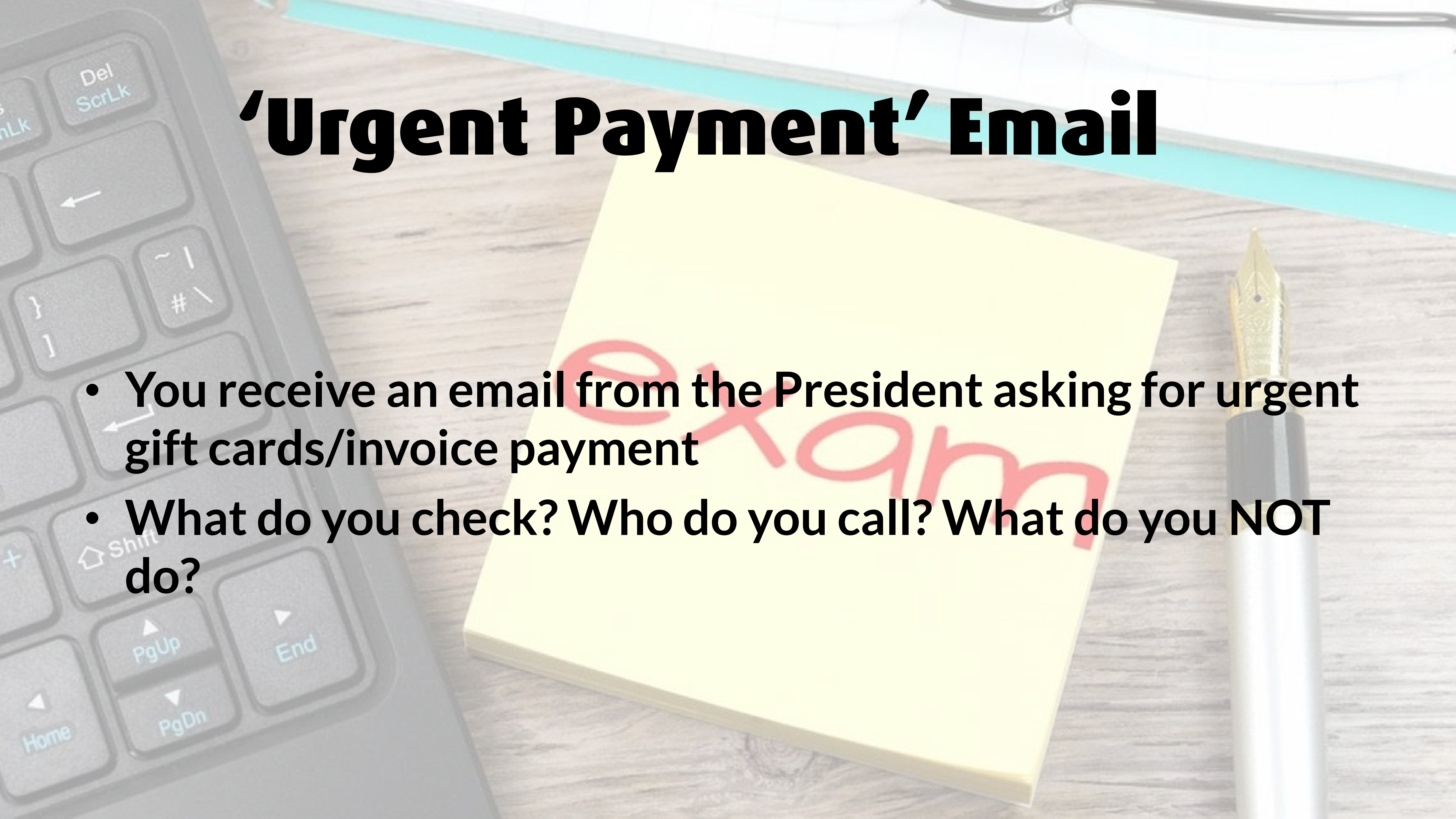
- Pause on urgent requests for money, gift cards, or data
- Use the ‘Report Phish’ button or forward to the help address
- Verify money moves by calling a known number—not the email

Habit 5
Safer File Storage & Sharing

- Use approved folders/tools; avoid personal email/drives
- Remove access when projects end; tidy old shares quarterly
- Label especially sensitive files and limit who can see them

If Something Happens First-Hour Playbook

- **Pause & preserve:** don’t delete, don’t pay; take a screenshot
- **Call the right people:** IT/security, supervisor, finance, comms
- **Contain:** if a device acts strange, disconnect Wi-Fi (don’t wipe)
- **Decide who needs to know now vs. later;** keep a simple log



‘Urgent Payment’ Email

- You receive an email from the President asking for urgent gift cards/invoice payment
- What do you check? Who do you call? What do you NOT do?

Let’s Summarize

In the world of fiscal services, what can you do that can make a big difference in ensuring a safer technology infrastructure?