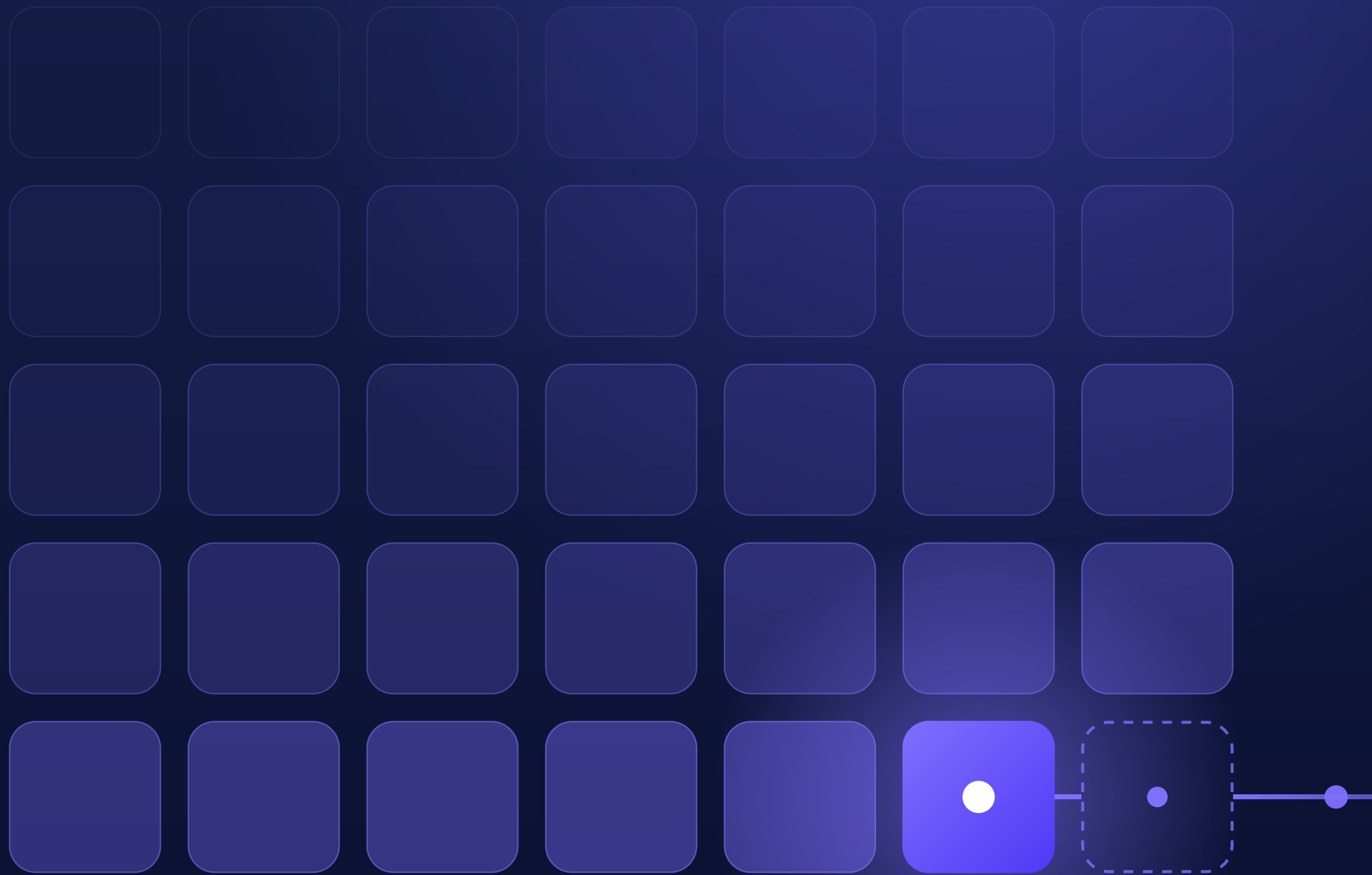




Make October the **start**, not the end

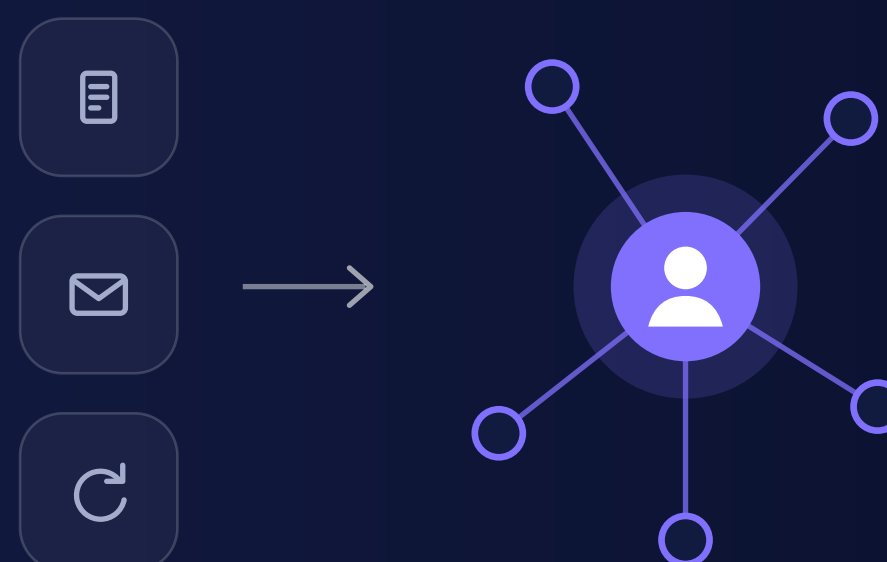
Cybersecurity Awareness Month gets people thinking about security. But awareness alone does not tell you where human risk exists, which people are most exposed or what needs attention first.

Go beyond posters, emails and refreshers

This October, go beyond posters, emails and annual refresher training. Use the month to:

- ✓ Measure what your people actually know
- ✓ Test how they respond to realistic phishing
- ✓ Identify exposed credentials
- ✓ Understand identity, hygiene and access risks
- ✓ Find where multiple risks combine around the same person
- ✓ Prioritize what to address first
- ✓ Track whether human risk improves over time

That is the shift from security awareness activity to **Human Risk Intelligence**.



Awareness as a one-month exercise misses the point

A typical Cybersecurity Awareness Month campaign might include awareness posters, employee emails, security training, a phishing simulation, and security tips and reminders. These activities can all play an important role in building awareness. The problem is what happens next.

A completion rate tells you who finished training. A phishing result tells you who clicked or reported. A breach check can tell you whose credentials have been exposed. Viewed separately, these signals only tell part of the story.

THE BIGGER QUESTION

Where does human risk actually exist across your organization?

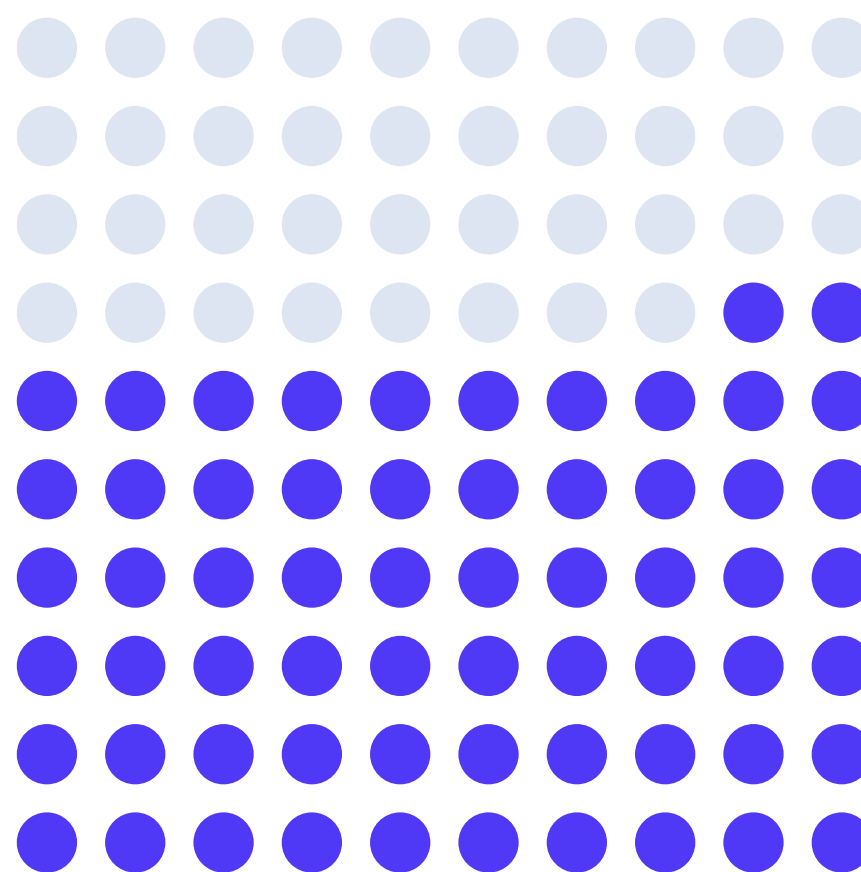
Answering that means moving beyond individual activities and understanding how different risk signals connect around each person.



62%

of breaches involved the human element in 2026, up from 60% the year before. Awareness is not a side issue. It sits inside most breaches.

Verizon 2026 Data Breach Investigations Report



Start by measuring what people actually know

Before assigning more training, establish a baseline. A knowledge assessment can show where understanding is already strong and where employees may need more support. Look across topics such as:



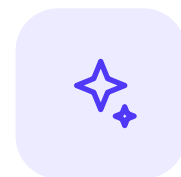
Phishing and social engineering



Password security · MFA ·
Data handling



Remote working ·
Physical security

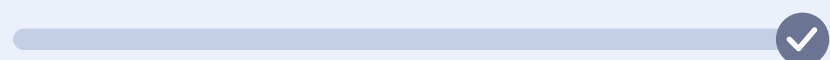


AI and emerging threats

Instead of assigning the same training to everyone, use those results to focus learning on the areas that need attention.

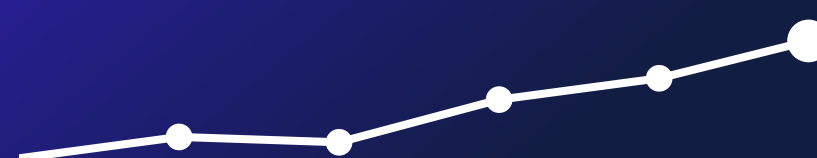
MOVE FROM

“Everyone completed the annual course.”



TO

“We know where awareness gaps exist and can track whether they improve.”



Test awareness in the real world

Knowing the right answer in a course does not always translate into safer behavior. Phishing simulations help you see what happens when employees encounter realistic threats in their inbox. Look beyond the click rate.

The important part is what happens after the simulation. Treat the result as another risk signal, not the whole story.

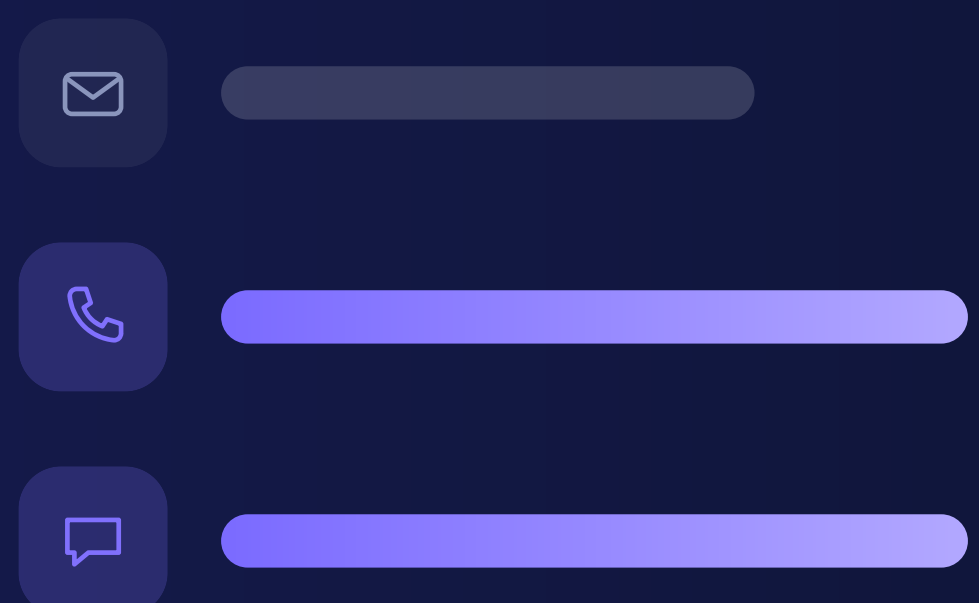
CONSIDER

- ✓ Who interacted with the simulation
- ✓ Who reported it
- ✓ Whether risky behavior repeats
- ✓ Whether behavior improves over time
- ✓ Which employees may need extra support

40%

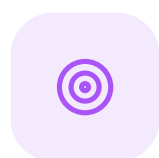
higher success rate for voice and text phishing simulations than email. Phishing has moved beyond the inbox, so testing needs to as well.

Verizon 2026 Data Breach Investigations Report



Human risk is not created by awareness alone

Someone can perform well in training and still represent significant risk if their credentials are exposed, MFA is missing or they have elevated access. A more complete view looks across four areas.



Target

How attractive is this person to an attacker?

- Seniority
- Department
- Financial responsibilities
- Access to sensitive information



Awareness

How well equipped are they to recognize and respond to threats?

- Knowledge assessments
- Training performance
- Phishing simulation behavior
- Reporting behavior



Hygiene

Are basic controls and habits reducing or increasing exposure?

- Credential exposure
- Password age
- Security configuration
- Other identity hygiene indicators



Access

What could happen if this account were compromised?

- Privileged roles
- Access to important systems
- Administrative permissions
- Authentication controls such as MFA



Together, these signals provide more context than a training completion percentage alone.

Find the risks that become more dangerous together

One weak signal may not require immediate attention. Several weak signals around the same identity can create a much more important risk. These are **Toxic Combinations**.

FOR EXAMPLE

Dormant account

+

Old password

+

No MFA

Each signal matters on its own. Together, they create a clearer priority.

High access

+

Exposed credentials

+

Weak awareness

That person may need attention before someone whose only issue is an overdue training course.

Human Risk Intelligence connects these signals so teams can understand where risk is concentrated, why it matters and where to focus first.

97%

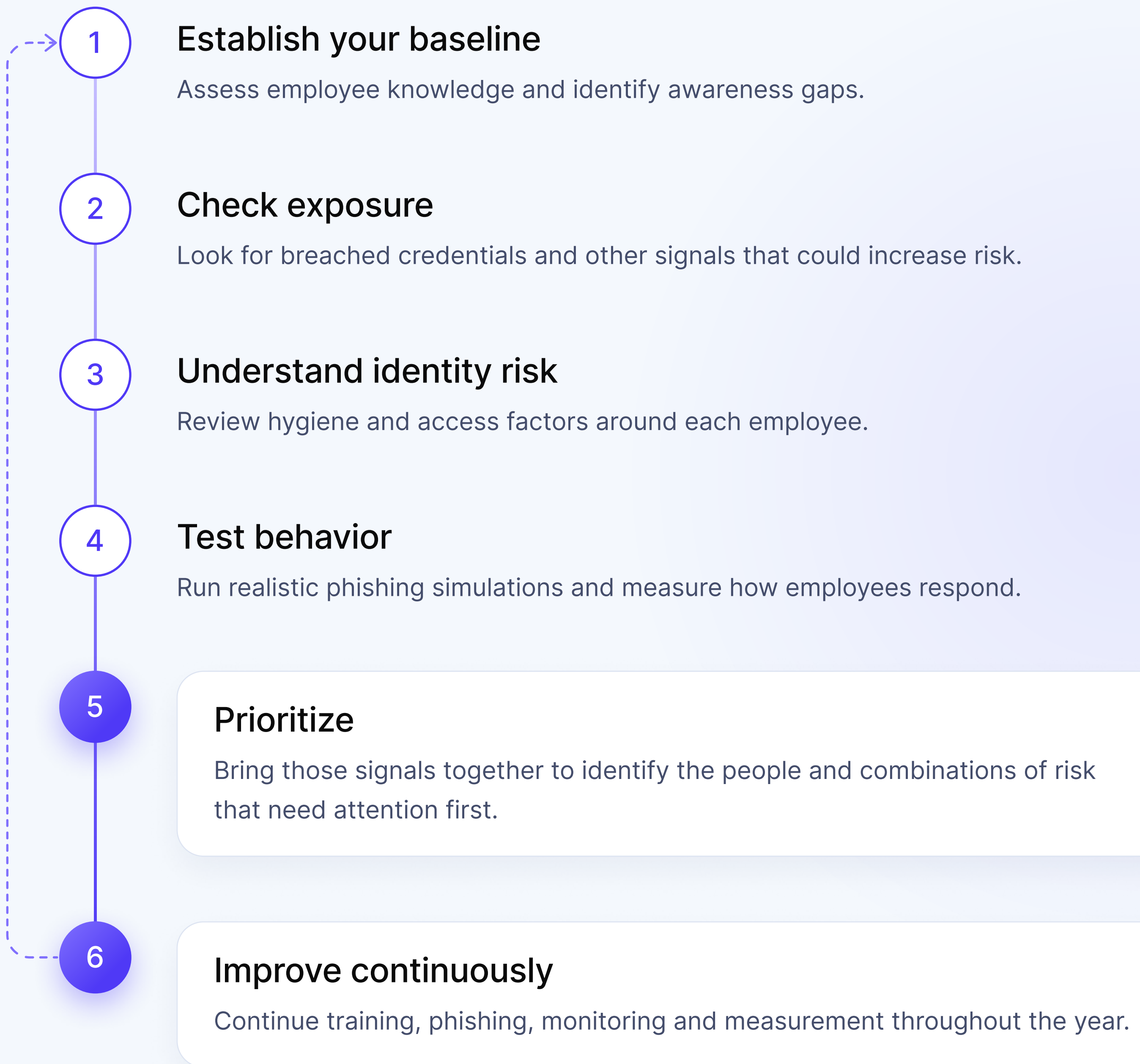
of identity attacks were password spray attacks. Exposed credentials and missing MFA are exactly the weaknesses that stack into a Toxic Combination.

Microsoft Digital Defense Report 2025

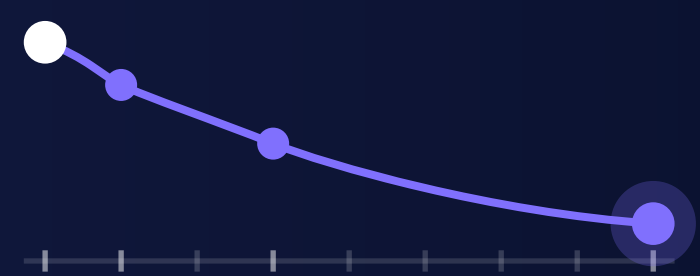
Think you can spot one?

Find the Toxic Combination →

Turn October into an ongoing human risk program



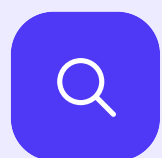
October gets the process started. The goal is to still be reducing human risk in November, January and June.



Your Cybersecurity Awareness Month checklist

Use this October to ask:

- ☐ Do we know which security topics our employees struggle with? 
- ☐ Have we tested how employees respond to phishing recently? 
- ☐ Do we know whether employee credentials have been exposed? 
- ☐ Do we know which people are more attractive targets to attackers? 
- ☐ Can we identify elevated access, missing MFA or other identity risks? 
- ☐ Can we see when several risk signals affect the same person? 
- ☐ Can we prioritize which people or risks need attention first? 
- ☐ Can we show whether human risk is improving over time? 



If you can only answer questions about training completion, there is more of the human risk picture still to uncover.

Put it into practice this October

With usecure, you can use Cybersecurity Awareness Month to move from periodic awareness activity to continuous Human Risk Management and Human Risk Intelligence. Start by:

✓ Running a knowledge gap analysis

✓ Launching realistic phishing simulations

✓ Checking for credential exposure

✓ Reviewing identity, hygiene and access signals

✓ Delivering targeted security training

✓ Bringing those signals together in uHealth

✓ Identifying Toxic Combinations

✓ Prioritizing what needs attention

✓ Tracking human risk over time

The underlying platform combines security training, phishing simulations, dark web monitoring and policy management. HRI adds the context that helps those signals make more sense together.

October is a moment. Human risk is year-round.

Prove it, don't just tick it.

Use Cybersecurity Awareness Month to train your people, test what stuck and find the gaps, then keep reducing human risk all year.

Get started free →

14 days. No credit card. Set up in minutes.

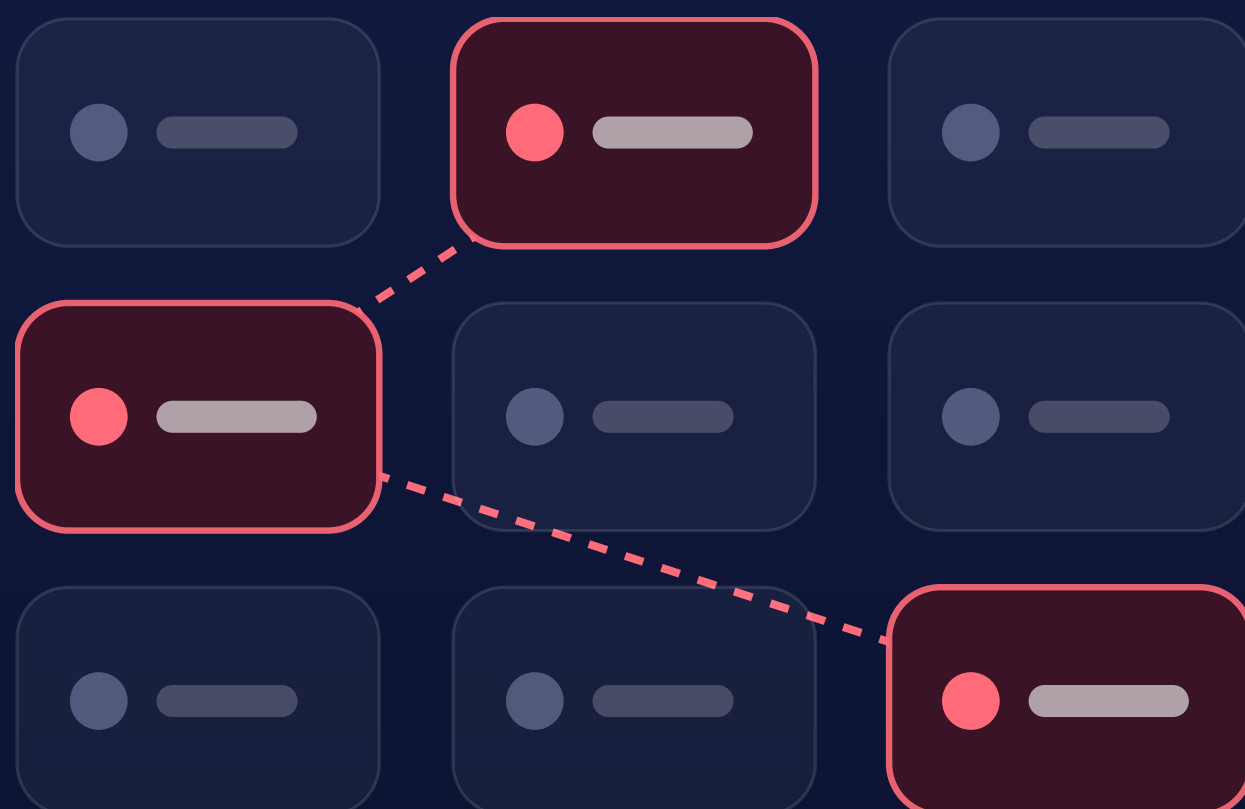
Free ways to get started this October

Not ready to start a trial? Put your security instincts to the test with two quick challenges.

CHALLENGE 01

Can you find the Toxic Combination?

One risk signal might not look urgent. Several around the same person can tell a very different story. Can you find the risky combination before an attacker does?



Play the Toxic Combination challenge →

CHALLENGE 02

Think you can beat Cyberto?

Phishing and social engineering are designed to make you act before you think. See whether you can spot the tricks used by our resident scammer.



Beat Cyberto →

Ready to measure your own human risk?

Assess awareness, test employees, uncover exposure and start building a continuous view of human risk.

Get started free →