

How to reduce employee phishing susceptibility

A Comprehensive Approach to
Human Risk Management



Table of contents

Executive Summary	03	Case Study	08
Introduction to Phishing	03	Conclusion	09
Growing Phishing Landscape	04		
The Cost of Phishing	04		
How to Assess Phishing Risks	05		
Interpreting Assessment Data	06		
Leveraging usecure for Phishing Risk Assessment	06		
Strategies to Reduce Phishing	07		



Executive Summary

The human element was present in 62% of breaches analyzed in Verizon's 2026 DBIR. But social engineering is also changing: simulated voice and text attacks achieved 40% higher median success rates than email-based simulations.

That makes phishing resilience more important, but also harder to measure through email click rates alone. An employee who fails a simulation may represent relatively limited exposure. Another employee with the same result may also have exposed credentials, missing MFA and privileged access. The behavior is the same. The risk is not.

Reducing phishing susceptibility starts with awareness, but it should not end there. Organizations also need to understand how phishing behavior connects with credential exposure, identity hygiene and access. This guide explores how to build phishing resilience while developing a clearer picture of human risk.

Phishing has moved beyond the inbox

Phishing is a form of social engineering designed to manipulate people into revealing information, credentials or taking an unsafe action. Today, those attacks extend well beyond traditional email. Common forms include:

- **Email Phishing:** Fraudulent messages designed to steal information, credentials or trigger an action.
- **Spear Phishing:** More targeted attacks tailored to a specific person, role or organization.
- **Vishing and Smishing:** Social engineering delivered through SMS, messaging apps or voice calls.

Attackers exploit human psychology, using urgency, authority, curiosity and fear to encourage people to act before they think. But phishing is also moving beyond the inbox. Voice, SMS and other social engineering channels are becoming increasingly important, while AI is making impersonation and tailored attacks easier to scale.

40% higher median success rates were recorded for simulated voice and text attacks than for email-based simulations.

62%

of breaches involved the human element, while social engineering represented 16% of breaches.

40%

simulated voice and text attacks achieved 40% higher median success rates than email-based simulations.

38%

of UK businesses experienced phishing attacks in the previous 12 months, rising to 60% of medium businesses and 63% of large businesses.





Phishing is changing, not disappearing

Phishing remains one of the most common ways attackers target businesses, but the techniques are changing. In the UK, 38% of businesses experienced phishing attacks in the previous 12 months, rising to 60% of medium businesses and 63% of large businesses.

Key insights from the breach:

- The leaked data primarily comprises usernames and password combinations.
- While much of the information stems from prior breaches, its availability in a single repository creates opportunities for cybercriminals to exploit.
- The breach reflects the growing sophistication of threat actors, who compile vast data sets for use in large-scale phishing campaigns.

Credential exposure can make social engineering more convincing and more damaging. But phishing risk depends on more than whether someone receives or clicks a message. Identity hygiene, authentication controls and the access attached to that account all shape the potential impact.

To reduce phishing risk, organizations need to understand both why social engineering works and what sits around the person being targeted.

The impact goes beyond the click

A successful phishing attempt can lead to:

- **Financial Losses:** Fraud, business email compromise and account takeover can result in direct financial losses.
- **Reputation Damage:** Compromised accounts can expose sensitive company, customer or employee information.
- **Operational Disruption:** Investigation, recovery and incident response can consume significant time and resources.

The same phishing behavior can have very different consequences depending on the identity involved. That is why phishing susceptibility should be treated as one risk signal, not a complete measure of human risk.

Why phishing still works

Why does social engineering succeed? Social engineering is designed to influence normal human decision-making, particularly when people are busy, distracted or under pressure. Common tactics include:

- **Urgency:** Pressure to act quickly can reduce the time someone takes to question a request.
- **Authority and trust:** Attackers impersonate executives, colleagues, suppliers and familiar brands to make requests appear legitimate.
- **Familiarity and context:** Relevant, personalized messages can be harder to distinguish from legitimate communication.
- **Channel switching:** Social engineering now extends across email, SMS, messaging apps and voice calls, making recognition more difficult.

Attackers increasingly combine these techniques with more convincing content and additional channels. Verizon found that simulated voice and text attacks achieved 40% higher median success rates than email-based simulations.

Recognize the pressure tactics

Common social engineering techniques include:

- **Urgency:** "Your account will be deactivated unless you act now!"
- **Fear:** "You owe back taxes; legal action will follow if unpaid."
- **Authority:** "This is the CEO—please process this payment immediately."
- **Opportunity or curiosity:** Using rewards, unexpected documents or topical events to encourage interaction.

Recognizing these techniques is important, but awareness alone cannot show how much risk a successful attack creates. The surrounding identity and access context matters too.

Start by measuring how people respond to realistic threats. Then connect that Awareness signal with credential exposure, identity hygiene and access to understand where risk is concentrated.



How to assess phishing risk in context

Phishing risk starts with how people respond to threats. But susceptibility alone does not show which identities create the greatest exposure. A stronger assessment connects phishing behavior with credential exposure, identity hygiene and access.

1. Establish a phishing baseline

- Measure how employees recognize, interact with and report phishing attempts to create an Awareness baseline.

2. Run realistic phishing simulations

- Test employees with varied scenarios, including credential theft, impersonation, urgent requests and malicious links. usecure's uPhish can automate and tailor simulations at scale.

3. Analyze behavior, not just clicks

- Track interactions, reports, credential submissions and repeat susceptibility.
- Look for patterns across roles, departments and access levels.
- Identify which tactics and channels are most effective.

4. Track change over time

- Compare results over time to see where phishing resilience is improving and where weaknesses persist. Use benchmarks for context, not as the definition of risk.

5. Add identity and hygiene context

- Review MFA, credential exposure and other identity hygiene signals. A phishing failure becomes more significant when it overlaps with other weaknesses.

6. Review previous incidents and exposure

- Look for recurring patterns across phishing incidents, reported messages, exposed credentials and user behavior.

7. Connect the signals

- Bring phishing behavior together with Awareness, Hygiene, Access and Target signals to identify which identities need attention first.

Human Risk Intelligence turns these separate signals into a clearer, continuously updated view of human risk.



Turning phishing signals into action

Phishing assessments are most useful when they help you decide what needs attention. Start with the behavior you observe, then add the context around each identity.

1. **Prioritize where risk is concentrated:** A high phishing score is one signal. Look at the identity behind it before deciding what needs attention.
2. **Target the awareness gaps:** Use assessment and simulation results to focus training on the topics and behaviors employees struggle with most.
3. **Add identity context:** Review credential exposure, MFA, hygiene and access alongside phishing behavior to understand the potential impact of compromise.
4. **Measure improvement:** Track reporting, susceptibility and recurring behavior over time to see where resilience is improving and where weaknesses remain.
5. **Look for combined risk:** Identify where weak Awareness overlaps with other signals around the same identity. These combinations can create a more urgent priority than any single signal alone.

The goal is not simply to reduce clicks. It is to understand where phishing behavior contributes to wider human risk and focus attention accordingly.

From phishing signals to Human Risk Intelligence

usecure helps organizations measure phishing behavior, strengthen awareness and connect those results with the wider risk context around each identity. uHealth brings these signals together through Human Risk Intelligence.

The process connects:

- **Phishing behavior:** uPhish tests how employees respond to realistic social engineering scenarios.
- **Awareness:** uLearn identifies knowledge gaps and delivers targeted learning based on employee needs.
- **Exposure and hygiene:** Credential exposure and identity signals add context around each user.
- **Access and Target:** Identity context helps show the potential impact and attractiveness of a compromised account.
- **Human Risk Intelligence:** uHealth connects these signals to show where risk is concentrated and where multiple weaknesses combine.

Instead of treating a phishing result as the final score, teams can see it in context, prioritize what needs attention and track how human risk changes over time.





Strategies to build phishing resilience

Make training targeted and measurable

Successful phishing training programs should:

- **Keep it relevant:** Use realistic scenarios that reflect the threats employees are likely to face.
- **Adapt to changing threats:** Update training as phishing tactics, channels and attacker techniques evolve.
- **Measure improvement:** Track knowledge, behavior and reporting over time to identify persistent gaps.

Keep awareness continuous

Phishing tactics change throughout the year, so awareness should not rely on a single annual course. To stay effective, training should include:

- **Regular learning:** Keep content relevant to new threats and employee needs.
- **Reinforcement:** Use short training, assessments and simulations to strengthen learning over time.
- **Shared responsibility:** Reinforce secure behavior across the organization, with leaders supporting consistent participation.

Use simulations to test behavior

Simulated phishing attacks, such as those facilitated by uPhish, enable employees to:

- **Test recognition:** See how employees respond to realistic phishing and social engineering scenarios.
- **Reinforce safer responses:** Repeated practice helps employees build confidence in recognizing and reporting suspicious activity.

Training and simulations improve Awareness, but they are only part of the picture. Connect those results with identity, hygiene and access signals to understand where phishing susceptibility contributes to wider human risk.





Case Study: How Winning Group Reduced Phishing Susceptibility by Over 90%

At a Glance

Winning Group reduced simulated phishing credential compromises from 9% to less than 1% within six months. Regular training and phishing simulations helped employees build stronger awareness and confidence in recognizing suspicious activity.

Using Auto Enrol, employees received regular security awareness training, supported by ongoing phishing simulations to measure how behavior changed over time.

The Challenge

As Winning Group grew, protecting customer data meant reducing the likelihood of employees being caught by phishing attacks. Early simulations showed that 9% of employees compromised their credentials, creating a clear baseline for improvement.

Aware of the increased risk of data breaches, especially as businesses grow and become more susceptible to cyber-attacks through human error, Winning Group faces the challenge of ensuring the escalating potential for mistakes don't compromise its fundamental mission of benefiting customers and communities

The Solution

Winning Group implemented usecure's human risk management solution, which included:

- **Regular Training:** Monthly video-based sessions via AutoEnrol to ensure consistent, accessible education.
- **Phishing Simulations:** Regular, realistic phishing tests to build practical experience in spotting threats.
- **Unified Risk Reporting:** Continuous monitoring of employee risk scores to track and manage vulnerability.



Results

The Winning Group's use of usecure significantly enhanced their security posture:

- Employee susceptibility to phishing reduced from 9% to less than 1% in six months.
- Implementing regular staff training decreased human phishing vulnerability by 90%.
- Enhanced staff proficiency in managing key cybersecurity challenges post-training.

After six months of training, another round of simulated phishing emails were sent out to staff. This time, less than 1% of employees compromised their credentials - a reduction of over 90% from only six months before

From Awareness to Human Risk Intelligence

Winning Group shows how phishing behavior can improve through continuous training and testing. Today, HRI takes that Awareness signal further by connecting it with the wider context around each identity, helping teams understand where risk is concentrated and what needs attention first.

[Read full case study here](#)



From phishing resilience to Human Risk Intelligence

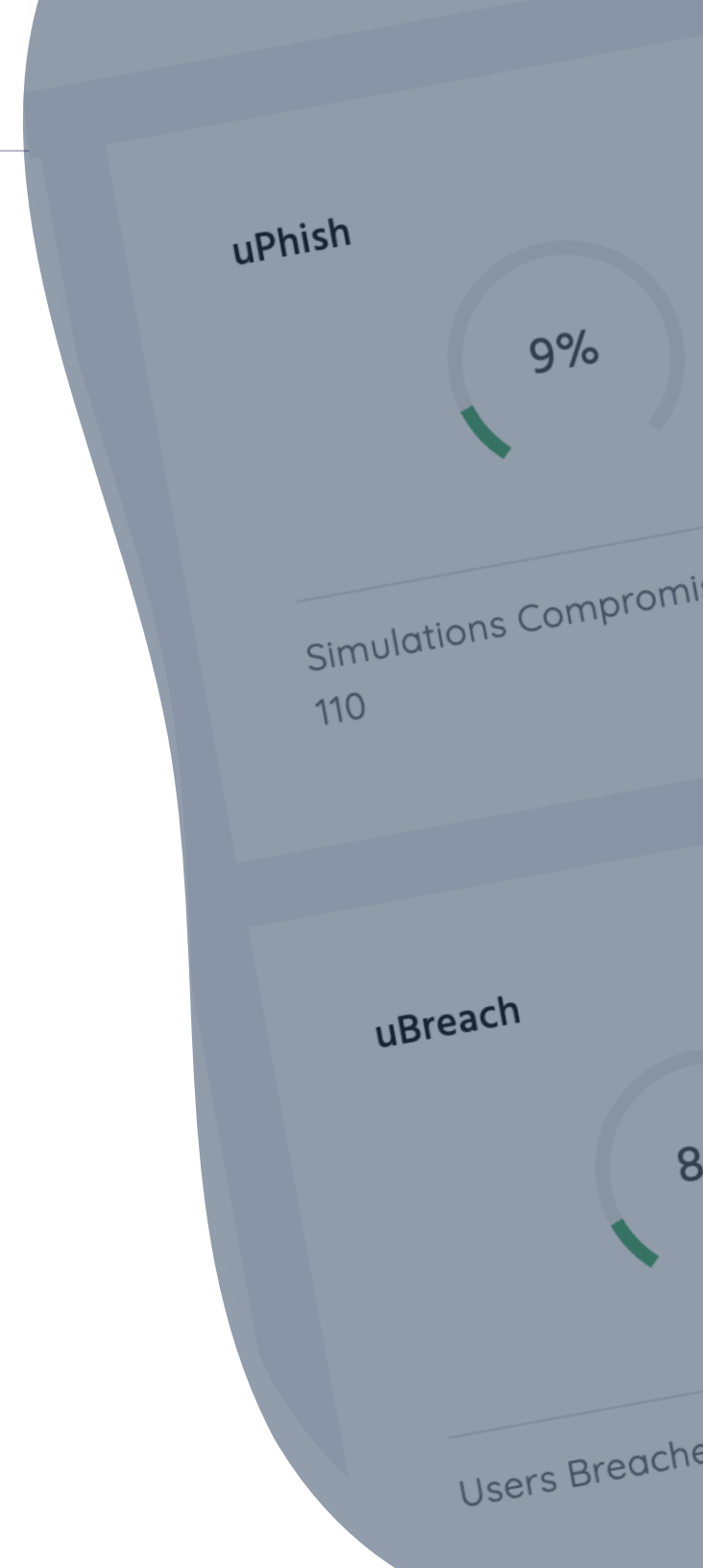
Reducing phishing susceptibility takes continuous training, testing and measurement. But phishing behavior is only one part of human risk. The next step is connecting that Awareness signal with identity, hygiene, access and exposure to understand where risk is concentrated and what needs attention first.

Keep reducing human risk

usecure brings security awareness training, phishing simulations, credential exposure and Human Risk Intelligence together in one platform, helping you move from isolated activity to a clearer, continuously updated view of human risk.

Ready to put it into practice? Start measuring phishing behavior, uncover wider risk signals and track improvement over time. **Get started free.**

Phishing resilience is an important part of the picture. Human Risk Intelligence helps you understand what that behavior means in context, so you can prioritize attention where it matters most.



Research and sources

1. [Verizon 2026 Data Breach Investigations Report](#)
2. Human element, social engineering and mobile phishing simulation data.
3. [UK Cyber Security Breaches Survey 2025/2026](#)
4. UK phishing prevalence and cybersecurity practices across businesses.
5. [APWG Phishing Activity Trends Reports](#)
6. Phishing, smishing and business email compromise trends.
7. [Microsoft Digital Defense Report 2025](#)
8. Identity attacks, password spraying and AI-assisted phishing trends.

Further reading

1. [Human Risk Intelligence](#)
2. [Toxic Combinations in Human Risk Intelligence](#)
3. [Winning Group: Over 90% reduction in phishing susceptibility within six months](#)

