Zoho eProtect

Admin's guide

Building a cyber-aware culture

ZOHO

Table of contents

Introduction

Often, the most secure organizations are those that foster a culture of security and center their organization's practices around secure emailing practices. Building a culture in which security takes precedence is one of the most crucial factors to ensure that your organization is protected from external threats. Threat actors most often prey on human psychology to manipulate and email recipients into trusting an email and engaging with them. This is the most common method through which cybercriminals perpetrate social engineering attacks.

In fact, human error has played a major role in 88% of successful cyberattacks. Therefore, it's the organization's responsibility to build a culture in which cyber awareness takes utmost precedence. Admins should encourage secure practices and ensure that senior management follows these practices, too.

This guide is designed to help you understand the importance of a cyber-aware culture and how admins can build one for their organization.

Human error has played a major role in 88% of successful cyberattacks.

Why is cyber awareness important?

Being cyber-aware helps an organization in many ways, ranging from better compliance with regulatory bodies to improving customers' trust. Let's take a look at some of these reasons.

1 Human error can't be averted

Humans are often the weakest links in any security context. With threat actors becoming smarter in creating attacks, it's possible that malicious emails or other forms of communication often slip through without the employee noticing. If they continue to engage with the content without realizing its nature, they put the entire organization at risk of a breach. Developing a security culture and providing sufficient training will make employees more aware of such scenarios.

2 It ensures compliance

Now more than ever, there's increased awareness about secure data handling practices. In fact, new regulations are created all the time to ensure that organizations are taking the necessary measures to handle their data safely. By creating a strong security culture, organizations can pass any audits that could be conducted on their company.

3 It leads to better technological awareness

Because newer threats and prevention methods are always evolving, educating users about the threats they face and the protection measures that have been set up is crucial. Employees should be aware of the software solutions that the company uses. This can be disseminated to users through a security awareness program to ensure compliance.

4 It improves brand reputation

Setting up a strong security culture and enforcing adherence to it will help your brand's reputation. If your company is a pioneer in following secure practices in a certain region or industry, your reputation improves, and this in turn increases your credibility.

5 It builds customer trust

When your customers select a brand to do business with, they consider many factors. Data security has become one of those deciding factors in going with a certain brand. When you publish information publicly about the practices followed and your employees' expertise in data security, they'll develop better trust and opt for your brand.

Key principles of a cyber-aware culture

A cyber-aware culture is shaped by everyday habits and the values leaders reinforce. By embedding these ideas in their policies, organizations strengthen security.

1 Leading by example

Security starts at the top. When executives and managers follow best practices such as using MFA, conducting thorough training, and promptly reporting suspicious activity, they signal that cybersecurity is a priority for everyone. Visible leadership involvement builds credibility and motivates employees to adopt safe behaviors in their own work.

2 Shared responsibility

Cybersecurity works effectively when everyone in the company considers it a collective duty. Every employee, from interns to senior leaders, plays a role in safeguarding data and systems. By emphasizing shared responsibility, organizations ensure that security becomes part of daily decision-making, reducing the chances of gaps or oversights that attackers can exploit.

3 Openness and trust

A blame-free culture encourages employees to report phishing attempts, accidental clicks, or security concerns without fear of punishment. When staff know their reports will be welcomed and acted on, potential threats surface faster and can be contained before causing damage, turning transparency into a powerful defense.

4 Continuous learning

Threats evolve constantly, so awareness efforts must keep pace. Ongoing training sessions and phishing simulations help employees stay informed about new attack techniques and reinforce safe habits. Continuous learning keeps security top of mind and equips teams to respond confidently to emerging risks.

How to build a cyber-aware culture

Implementing a security culture for your company is most effective when it's done in a phased manner. Let's discuss the process that many organizations have found to be most effective.

1 Draft your security policies

Based on your assessment of your company's needs and your employees' current awareness levels, you can draft new policies and guidelines. Incorporate all aspects of security into your policy to ensure that there are no gaps and no aspect of your cybersecurity plan is left overlooked. Be very specific about what policies and practices you'd like employees to follow.

A minute level of specificity helps build a strong security culture because it will require certain behavioral changes from your employees. Knowing exactly what needs to be done in certain situations helps them follow the outlined guidelines and policies.

2 Policy announcement by leadership

How you choose to announce these policy changes makes a huge difference in how effectively it's followed across the company. Making a bit of noise about it and leading by example ensures that employees welcome these changes with the required amount of seriousness and excitement.

Senior management should convey how these decisions were made, with clear explanations of any changes to current processes. IT admins can implement policies for management first, and then use specific scenarios to educate users about how the policies have bettered their security posture. You can also impart information about how these changes have helped avert any threats that the company may have faced.

During the announcement, management should also inform employees who the person in charge of security will be and what authority they have so that there's no confusion going forward.

3 Formulate customizable training plans

Once changes about these assessments have been communicated to your employees, organize workshops and training sessions to impart the required knowledge needed to follow these practices. Make them as engaging as possible to ensure participation from all of your employees. Without overwhelming them with too many new things, start slow and introduce them to the policy decisions in a phased manner. This helps them implement the new practices one by one.

Ensure that the material used in the training is available in a central repository so that employees can refer to it when they have a question or they're not sure what to do in a specific scenario.

4 Stress the positive impact and repercussions

Building a cyber-aware culture works best when employees clearly see both the benefits of secure behavior and the risks of neglecting it. Highlight how safe practices protect sensitive data and keep business operations running smoothly. Celebrate successes, such as a department spotting a phishing attempt early or completing training with high scores, to show that individual actions positively impact the organization's security posture.

At the same time, be transparent about the real consequences of careless behavior. Explain how a single click on a malicious link can lead to data breaches, financial loss, regulatory penalties, or reputational damage that affects everyone's work. Communicating these potential repercussions is about helping employees understand the stakes and empowering them to make smart decisions that safeguard both their own work and the company as a whole.

5 Encourage and handle user reports

Creating a strong cyber-aware culture depends on how effectively employees can report suspicious activities without hesitation. Providing clear channels such as dedicated email addresses, internal portals, or reporting tools for phishing attempts or unusual behaviors is key. Promptly acknowledging these reports and communicating the actions taken reinforces trust and shows that their vigilance drives meaningful outcomes.

Beyond making reporting easy, organizations must treat every report as an opportunity to improve security defenses. Regularly sharing anonymized insights from user reports can help the wider workforce recognize emerging threats. This not only encourages consistent participation but also cultivates a proactive mindset where employees feel empowered to be the first line of defense.

6 Foster a no-blame culture

Fear of punishment discourages employees from admitting mistakes or reporting incidents, often allowing threats to linger unnoticed. Establishing a no-blame culture shifts the focus from fault-finding to problem-solving. When staff know that accidental clicks or missteps will be met with support and education rather than reprimand, they're more likely to come forward quickly, enabling faster containment of risks.

7 Reward and review regularly

Positive reinforcement motivates employees to practice safe cyber habits consistently. Recognizing individuals or teams who identify threats, report incidents, or excel in security training builds morale and reinforces desired behaviors. Rewards can range from public acknowledgment to small incentives, creating a culture where cybersecurity is celebrated rather than treated as an obligation.

8 Monitor performance and iterate

Cyber threats evolve constantly, and a successful awareness program must evolve with them. Tracking key metrics, such as phishing test success rates, reporting frequency, and training completion, reveals the effectiveness of current strategies. These insights help identify weak points and iterate policies to ensure that the training imparted to employees remains relevant and impactful.

The role of eProtect in enhancing email security

While it's important to build a cyber-aware culture to ensure that your employees stay vigilant, it's also crucial to implement a robust email security solution for your company. This serves as an aid to your employees by detecting threats that are invisible to the human eye.

Zoho eProtect is an email security solution that's built to provide enterprise-grade threat protection for all organizations, irrespective of the email provider that you've hosted your email with.

With eProtect, you get:

Advanced threat protection against phishing, spoofing, malware, and zero-day attacks.

Multi-layered filtering to block malicious attachments, links, and spam before they reach the inbox.

Real-time monitoring and threat intelligence to identify and stop evolving attack patterns.

User behavior analysis to detect account compromise, insider misuse, and negligent activity.

Detailed threat reports and insights that help IT teams understand attack trends, spot vulnerabilities, and make informed security decisions.

Easy integration with your existing email infrastructure for seamless deployment.

Conclusion

A truly cyber-aware culture thrives on empowerment, not enforcement. It's about creating an environment where people feel confident to question, report, and learn, because every alert raised, every suspicious email flagged, and every lesson absorbed adds a layer of protection. Rather than relying solely on firewalls and filters, this approach turns everyday employees into an active, adaptable defense network.

This guide was released by Zoho eProtect as part of Cybersecurity Awareness Month 2025. eProtect is a cloud-based email security and archiving solution that provides advanced threat protection for all on-premise and cloud email accounts. eProtect is the security solution powering Zoho Mail, a platform trusted by millions of users.

Knowledge is the first step.
Protection is the next.

Discover how Zoho eProtect secures your email →