Empowering Individuals for Enhanced Identity Protection

Ninoslava Bogdanovic, Share Foundation

Although cybersecurity may appear to be primarily a technological concern, it ultimately revolves around human being**s. Humans play a pivotal role in cybersecurity, as they can unintentionally compromise sensitive information** and systems through social engineering tactics or errors, emphasizing the need to empower individuals with appropriate technologies and awareness training.

In addition to the challenges posed by advanced attackers and the technical aspects of implementing multi-factor authentication (MFA), the true obstacle lies in inspiring individuals, both in personal and professional settings, to embrace this crucial security feature. Unfortunately, numerous reports suggest that businesses and individuals are not fully leveraging the potential of MFA.

While 56% of businesses claim to have implemented MFA. Shockingly, only 8% of C-suite executives utilize MFA across their various applications and devices. However, the issue extends beyond the corporate realm. Even social media users neglect best practices to safeguard their online accounts and personal information. For instance, a mere 2.6% of Twitter users have activated MFA for their accounts.

Several reasons contribute to this risky behavior:

1. Implementation and integration challenges: The complexity of incorporating MFA into daily business workflows makes it a daunting task.
2. Ineffective communication: The importance of implementing MFA fails to resonate effectively with businesses and society.
3. Misconceptions about cybersecurity: Some individuals hold beliefs such as "it won't happen to me" or "I have nothing to hide," undermining the perceived need for MFA.
4. Fear and uncertainty: The intimidating nature of cybersecurity alienates people from actively engaging in protective measures.

To address these concerns, it is vital to recognize that cybersecurity is not solely reliant on technology or processes. While technology can only offer a certain level of protection, employees can provide the contextual understanding necessary to detect and prevent attacks. By providing the right tools, knowledge, and support, organizations can unlock the full potential of their workforce and create a culture that embraces and maximizes the advantages of technology.

It is important to empower people in cybersecurity and identity protection to harness the benefits of digital technologies. Here are some strategies for achieving this goal:

Cultivating a Digital Mindset:

To empower individuals, it is crucial to foster a digital mindset within the organization. This involves developing an organizational culture that embraces technological advancements, encourages experimentation, and promotes continuous learning. By emphasizing the value of technology and its potential to drive positive change, employees are more likely to adopt new tools and approaches, becoming active participants in digital transformation.

Cultivating a Cybersecurity Mindset:

To safeguard our digital identities in today's interconnected world, empowering and engaging individuals in cybersecurity is paramount. Every organization possesses a security and organizational culture that should be transformed into a positive and proactive one. Blaming individuals for mistakes is counterproductive. Merely bombarding people with more technology exacerbates the situation by introducing unnecessary complexity. Instead, we should foster a culture that celebrates small victories. By focusing on all three domains of cybersecurity—people, processes, and technology—our businesses and societies can become safer and stronger.

Providing Training and Development Opportunities:

Investing in training and development is key to empowering employees to leverage technology effectively. This includes offering comprehensive training programs, workshops, and resources that equip individuals with the necessary skills to utilize technology tools and platforms efficiently. By providing ongoing learning opportunities, organizations enable employees to stay updated with the latest technological advancements and leverage them to enhance their work processes. Security awareness training should not solely focus on the "why" (the consequences of a breach), but also on the "why me?". The "why me?" aspect, provides individuals with the context needed to comprehend the relevance of cybersecurity to their own lives. Without this understanding, it becomes challenging to influence people's intrinsic motivation, which is key to driving behavioral change. Understanding the reasons behind certain behaviors, or the lack thereof, is crucial for impactful awareness training.

Tailoring Technology Solutions to Individual Needs:

Recognizing that each employee has unique requirements and preferences, organizations should strive to offer technology solutions that cater to individual needs. This can involve providing a range of tools and platforms to choose from, allowing employees to select the ones that align best with their work style and objectives. Customizable interfaces, flexible application integrations, and personalized user settings empower individuals to optimize their technology experience for enhanced productivity.

Empowering individuals to leverage the benefits of technology is a powerful strategy for organizations aiming to thrive in the digital age. By cultivating a digital mindset, cybersecurity mindset, providing training and development opportunities, tailoring technology solutions, encouraging collaboration, emphasizing automation benefits, and fostering innovation, organizations can create an environment where individuals feel empowered to harness technology to its fullest potential.

If you want to learn more about multi-factor authentication and how your organization can successfully and effectively deploy MFA, download our latest paper, "Selecting A Multi-Factor Authentication Solution: How to Address the Human and Technology Concerns."