Enabling people as the solution

Emails are our biggest vulnerability. Cyber Security covers a wide range of products and solutions for different threats, yet 91% of all cyber-attacks begin with a phishing email to an unexpected victim (Deloitte). An average employee sends and receives 126 emails per day – a number that is increasing with 3% on a yearly basis. If you would translate this into hours, this would account for roughly 3 hours a day, which in turn means that the average professional spends 28% of the workday reading and answering email. (The Radicati Group Inc from 2019). Cyber criminals are aware of that fact; email threats are morphing at scale and millions of new email phishing attacks are being crafted and sent every day.

Cyber professionals and chief security officers know this and are therefore taking different approaches to Email Security. Most of them, however, do not rely on their employees to take action and have put automated reporting systems or static warnings in place. The most common ways to tackle Email Security is to have a Security Email Gateway in place, along with awareness programs for those emails that security officers know that will pass their automated defense. Some companies integrated a **report button** in their O365 ribbon; When employees suspect an email, they report that email to security with a single click. Other may have static warnings, like the [EXTERNAL EMAIL] banner. The assumption is that it will raise the awareness of employees about the risks of emails coming outside their organization network. However, if you are a company representative dealing with external communication all day, the banner that appears in every correspondence will eventually lower your awareness and increases risks.

Time is of the essence

We know that our Security Email Gateways are penetrable. Once a phishing email passed through the SEG, it becomes a ticking time bomb in your employee inbox. Once security has detected, it takes them some time to analyze it and eliminate the threat. They will probably take different factors into account, such as sender authenticity, server location, return path and other vectors to mitigate that security incident. Once an email is declared a phishing email, system administrators will check their records to learn how many mailboxes were infected before finally removing the threat. Removing every phishing incident manually is time consuming and, in some cases, impossible. After an employee receives a phishing email, there is the possibility that they will fail to spot it is such. This means that it is only a matter of minutes from the moment that email landed in an inbox within your organization, until it is clicked and jeopardizes it. But what if your employees could respond in real-time incidents - even the most sophisticated ones?

IRONSCALES
World's 1st *Automated Phishing* Prevention, Detection & Response Platform

Ironscales is the first automated phishing prevention, detection, and response. Ironscales acts as a personal AI security assistant to each and every one of the organization's employees, located at mailbox level it actively scans and protects the employees mailbox. It learns employee's behaviour, and concentrates on who is sending and how relationships are built. By using

machine learning to learn behaviour and relationships, Ironscales detects at mailbox level Unlike static banners that appear every time an external email lands and are disregarded, Ironscales lights an indicative banner that only appears when a threat emerges, and with a built-

in report button to send it immediately to security check. Reporting employees receive an immediate notification of their actions. Reporting will create a series of events, not only security is informed but all affected recipients as well. Other recipients are notified that this email has been reported so they avoid falling in the same trap

Wisdom of the crowd / Centralized vs de- Centralized

Most SEGs need to be updated regularly to get familiarized with new threats that are based on signatures and rules. Ironscales' federation module uses community to learn and update new threats in real-time throughout the entire Ironscales network and does not require constant updates. This means that any attack that took anywhere around the globe is fed into the system, thus saving time of discovery and remediation of phishing emails. Auto-classification insures that employees do not received affected emails, those land at the security analysts for further mitigation.

Themis, the Ironscales AI assistance is given to security analysts as well where they can determine upon confidence levels whether an email is a phishing attack, span or false positive. All information is presented to security professionals in a way that they can take quick decisions and shorten valuable mitigation time; Moreover, all recipients of a particular email are presented and can be removed or restored in one click, saving system administrators valuable time as well.

The bottom line

Bad Actors: Phishing attacks are becoming much more sophisticated. One way you can help prevent malicious emails entering an employee's inbox, is to have a better understanding of the types of emails that person receives on a day-to-day basis. If your platform is personalizing your security based on the individual, you have a better chance of noticing which emails are not supposed to be there.

Humans are the Solution, Not the Problem: For years there was an idea that humans could not detect bad actors, or prevent phishing attacks. Instead, there was an overreliance on technology. If you simply rely on technology, your system will fall behind very quickly. Instead, deploy an active and passive platform that is continually learning while also gaining insights from its user.

Decentralized: Centralized solutions are dependent on data points and research from one specific source. In order to have a system that can detect and prevent multiple types of bad actors, you need a decentralized approach that can gather research from multiple sources.

Time: Ironscales enables security officers to move away from dependency of employees discovering phishing emails based on their knowledge. Employees are protected directly at their inbox level saving them valuable time while lowering the risk of unnoticed phishing mail

attack; Moreover, Ironscales brings a great return on investment in mitigation and remediation time

Do a free 90 day scan back now to see how your security is doing

Do you think your email security is doing a great job? We offer a 90 day scan back, you will be surprised how many emails passed your gateway.

Please take few minutes and visit https://www.mkbcyber.com/email-security