**Team Diversity with RMIT CIC and AWS Launches Shield CyberGames & ShieldSet**

**AUSTRALIAN FINANCIAL REVIEW – 1st November 2021 –** Through ransomware attack simulation and guided ethical instruction, [Shield CyberGames & ShieldSet] provides dynamic interaction for Neo-banks or Fin-Tech companies to improve cyber awareness and ethical responses to ransomware. Ethical experience with live cyber-attacks is now safe through Team Diversity’s recently launched [Shield CyberGames & ShieldSet] simulating the process of well-known attacks such as REvil, Sodinokibi, WannaCry, Petya and Bad Rabbit.

In 2018, Accenture reported the average cost of cyber-attacks at $13 million USD, listing banks as enduring the highest average annual cost at $16.37 million USD. The report stated 75% of companies infected with ransomware have up-to-date endpoint protection and 50% of security professionals state their organisation is not prepared for ransomware attacks. In 2020, 2,500 ransomware attacks were reported to the FBI, and ransom payouts totalled $350 million USD in cryptocurrencies Furthermore, Purplesec estimate by 2021, every 11 seconds a business will fall victim to ransomware, with 40% choosing to pay the ransom. With total costs from ransomware by 2021 at $6 trillion annually. In response to escalating costs of ransomware and a recent attack by REvil cybercriminal network, affecting 200 banks and demanding ransom of $70 million USD in Bitcoin the Biden Administration has sanctioned dealings with cryptocurrency exchanges which facilitate the payment of ransoms. Frustration among internal security departments and management provides opportunity through initiation of a culture shift promoting the simulation of cyber-attacks to educate for ethical cyber awareness. With an estimated 93% increase in ransomware in the first half of 2021 when compared to the first half of 2020, cyber awareness has never been more necessary.

[Shield CyberGames & ShieldSet] are designed for users of all levels of cybersecurity knowledge. Through the simulated cyber-attacks, users learn proactive ethical cybersecurity measures. Team Diversity aims to provide this value through experiential and adaptive learning. The cyber-attack simulations in [Shield CyberGames & ShieldSet] will provide proactive knowledge for all Neo-banks and Fin-Tech employees; ensuring organisations are cyber-ready, enhancing problem-solving skills when dealing with breaches, and build confidence. The games are designed to test the user for existing knowledge and place the user into the attack simulation which best suits their existing skillset. At the end of the game the user is directed to the appropriate learning modules designed to advance the users skillset. Scoring of ethical responsibility awareness and simulation responses are available for the security executives to track employee performance.

Continually updated ransomware attack simulations deliver experience with real-world cyber security issues. Moreover, [Shield CyberGames & ShieldSet] guide the player through being attacked, allowing the player to gain genuine experience from a safe cyber environment. Playing a responsive role of defender, players are guided through in-game-hints to deal with the attacks. [Shield CyberGames] are a subscription service offering ethical simulation of ransomware. [ShieldSet] includes the games with advanced training modules tailored using game results.

Prime Minister Boris Johnson’s office has released a statement which further iterates the importance of cyber security, “the [national security strategy] review will set out the importance of cyber technology to our way of life - whether it’s defeating our enemies on the battlefield, making the internet a safer place or developing cutting-edge tech to improve people’s lives.”

**Kelsey – FinTech CTO –** “Training my staff in the importance of cyber hygiene and ethics has never been easier. Now with the [Shield CyberGames and ShieldSet] from Team Diversity, I have a way of measuring my staff's awareness levels, I can direct the staff to the proper training they need, and I can reward those staff members who are always ethical and respond well with incentives. The games are fun and interactive. With regular updates which draw parallels to real-world attacks, my staff can live in the hot seat of a real attack from the safely of a simulated environment.”

**Call To Action -** <https://www.shieldcybergames.com/subscribe>

**FAQs**

**(Frequently Asked Questions)**

**CUSTOMER FAQs:**

1. **I don't know much about cyber-attacks. Will this help my knowledge?**

Yes. Our games are designed to be a fun and entertaining way to learn everything about cyber-attacks and how they work. We also supply easy-to-read modules which will equip you with all the information you need to know about cyber-attacks, how to respond to them and how to gain excellent scores in your games!

1. **I'm a busy person. Why should I invest my time in learning about cyber-attacks by playing these games?**

Cyber-attacks are a genuine issue today. It is just as important as and equal to protecting oneself from physical attacks. Ransomware is one of the most executed cyber-attacks. One of the most recent ransomware attacks was the REvil ransomware attack, that affected breached a software company names Kaseya, which had an adverse effect on banks across the world. The hackers demanded 70M dollars to end this attack. Many affected businesses were shut down for weeks. This shows the intensity of loss due to cyber-attacks. Our games are the best way for you to be well equipped with the knowledge and awareness you need to ensure you and your organization is safe from such losses.

1. **What is Ransomware?**

Ransomware is one of the many forms of cyber-attacks, where a hacker will steal and withhold your online data and will negotiate the release of it in exchange for ransom.

1. **Why should I care about cyber-attacks?**

These days, everyone is exposed to online platforms, and this factor directly involves cyber-attacks. Cyber-attacks have, unfortunately, become prevalent in our everyday activities as we all use the internet for our performance. Cyber awareness is important to ensure all your data stored online is safe from malicious agents who try to steal and misuse your information, or in the case of Ransomware, negotiate for ransom in exchange for you information.

1. **Do I need to be tech-inclined to access this?**

No. Our games are designed to be extremely user-friendly, where anyone can easily access and play the games, with a benefit of learning a lot about and be aware of cyber-attacks.

1. **Can I trust this?**

Yes! Our games are consciously sourced from a various of real-life and hypothetical situations which prepare you to be safe in this world of excessive cybercrimes.

1. **How does this prevent ransomware?**

We are determined to provide a safe and fun learning environment through our games to prevent ransomware by virtually putting you in situations where ransomware could take place. Our modules provide you the knowledge to ethically respond to such ransomware threats and entering the same responses in the games will ensure that you know how to deal with ransomware, thus preventing it.

1. **Why do I need this?**

Our games are perfect for you if you want to learn about cyber-attacks and prevention, without it being boring. If you want to be ready when faced with real-life situations of cyber-attacks, then you definitely need this!

1. **Will this make my life easier?**

We live in a world where technology has enabled a quick and smooth operation of our daily routines. Our games are designed to fit into your life without being time consuming and are a fun way to learn about cybercrimes, which, unfortunately, we all are under the constant threat of.

1. **What are modules? How are they helpful?**

Our modules are the ultimate online guides for cybercrime prevention. They provide all the information and knowledge about cybercrime and provide insights into various real-time situations. At the end of each chapter, we have quizzes so that you gain confidence in your cybercrime prevention skills. Using adaptive learning, modules may be skipped, or have more focus put on it based on how someone performed in the game and knowledge check.

1. **How much does the subscription plan cost me?**

You can subscribe to our games at an annual rate of AUD $250 per 10 employees. You can also subscribe to our ShieldSet (strongly recommended), which includes a yearly subscription to our games and modules for AUD $350 per 10 employees.

1. **How do we subscribe to this?**

It's simple. Log into our website <https://www.shieldcybergames.com/subscribe> and create a free account, choose a suitable subscription plan and you will be able to access your purchase at once!

1. **What values do the games contribute to?**

We designed our games with the intention to generate awareness, knowledge, and prevention of cybercrimes.

1. **Why do you update the games and modules?**

Cybercrime is constantly evolving. There isn't a "right way” of cybercrime occurrence, as it can take place at any place, any time, in any form. We want the games and modules to be a way of keeping up with real life and new cybercrime situations so that you are fully prepared for when it happens to you.

1. **How will you train the employees through games?**

Our modules are designed for everyone, regardless of their technological knowledge. We have various levels of difficulty for your employees to progress through. While our modules provide all the knowledge they need, our games are the ultimate testing platform for their knowledge and capabilities to think outside the box.

1. **What is the benefit of automated scoreboards?**

Automated scoreboards track the performance of each employee, displaying the scores of their games. These scoreboards are for users to track their progress and for security executives to gain better insight into employee's abilities.

1. **What is an attack simulation?**

This process involves having the user interact with an infected virtual computer. Allowing the user to gain experience with ransomware in a safe environment. The user is guided through responses to the ransomware by an in-game helper.

1. **How do the games address the needs of all user levels within a company?**

The responses of the user submitted into the game are tallied and scored. This score range will aid in directing the user to the appropriate training modules suited for their experience level.

1. **How do different user knowledge levels interact with the games?**

The games are designed for each level of technical ability. Depending on the role of the employee within the organisation they will be given different games. As awareness levels develop for employees, they will be given more challenging games accompanied by more intensive training modules.

**STAKEHOLDER FAQS:**

1. **Is this profitable to implement?**

Absolutely. Our games are the most reasonable and the best of their kind in the market. We work hard to ensure that your employees across all levels and departments are equipped with the knowledge they need to be cyber aware and keep your organisations safe at affordable prices.

1. **How will it fit into my business values?**

If your business values revolve around maximum profits, keeping the security and privacy of your organization and customers first, then we are the right choice for you. We give utmost importance to profitability and generating intelligence, ensuring everyone has the best experience with us.

1. **Does the government approve of this project?**

Yes! The government has sanctioned our games and modules as we made sure that they follow the relevant rules, regulations and laws evolving around cybercrime and prevention.

**VISUALS**



