ISSP

ISSP Training Center

Розвиток навичок кібер гігієни

www.issp.com

Користувач є найслабшим елементом у системі кібербезпеки будь-якої організації. Система кібербезпека повинна працювати з урахуванням ризиків кожного користувача окремо та симетрично реагувати на відповідні загрози. ISSP пропонує унікальну комплексну програму з підвищення обізнаності працівників у сфері кібербезпеки та розвитку навичок кібергігієни.

ЩО НОВОГО?

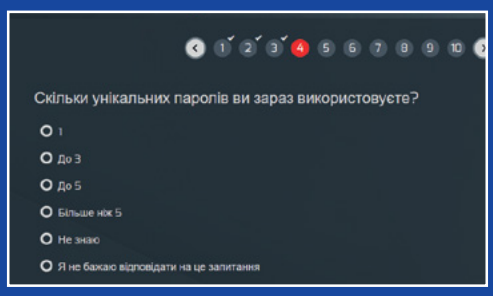
Результати перших етапів програми дозволяють з'ясувати зони ризику окремих працівників, цілих підрозділів та всієї організації, що надає організації можливість управляти кіберзагрозами в контексті як організації в цілому, так і окремих працівників. Такий підхід, у свою чергу, уможливлює ефективну реалізацію політики безпеки та прийняття виважених рішень про виділення інвестицій для подолання кіберзагроз.

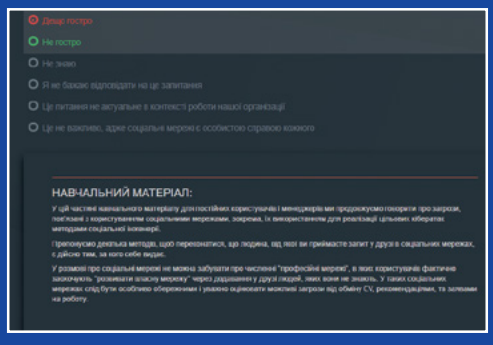
ЩО ОСОБЛИВОГО?

Комплексна програма з підвищення обізнаності працівників у сфері кібербезпеки складається з багатьох компонентів, а основна технічна платформа для передачі знань та оцінки залишкових кібер-ризиків співробітників розроблена на основі проекту, реалізованого в 2015-2017 роках Міністерствами оборони Естонії та Латвії в якості відповіді на цілеспрямовані кібератаки. Технічна платформа Cybexer надає інтерактивний інструмент, що складається з навчального модулю та двох модулів тестування поведінки користувачів у кіберпросторі.

5 складових програми

- Тестування поточного рівня кібергігієни всіх працівників на онлайн-платформі CybExer
- Навчання працівників за програмою Cyber Hygiene в автоматичному інтерактивному режимі, 3 рівні
- Періодична перевірка результатів навчання шляхом симуляції справжніх фішингових атак
- Цільові тренінги від досвідченого інструктора для користувачів із груп найбільшого ризику
- Регулярна комунікаційна підтримка і стимуляція





Тестування поточного рівня кібергігієни на платформі CybExer

- Програма націлена на три категорії працівників: керівників, звичайних користувачів та IT спеціалістів (з урахуванням їхніх знань IT), і сприяє усуненню загроз у поведінці представників кожної з цих категорій;
- Тестування і навчання побудовані на основі аналізу щоденних ситуацій із використанням комп'ютера та іншої портативної цифрової техніки;
- Тестування неможливо «пройти» або «не пройти» - усі працівники отримають власні профілі з кібергігієни із зазначенням унікальних для них зон ризику в кіберпросторі.

Навчання з кібергігієни на платформі CybExer

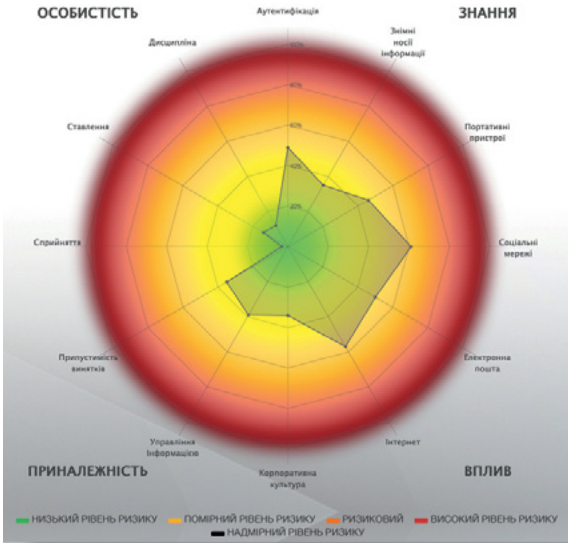
- Можливість проходити навчання і тестування будь-яку кількість разів із зручною для себе періодичністю;
- Програма регулярно оновлюється з урахуванням нових глобальних, національних або галузевих загроз;
- Навчання проходить в супроводі тренера, проектного менеджера і технічних спеціалістів.

Проведення цільових тренінгів з кібербезпеки

- На основі поточного рівня кібергігієни визначаються працівники з найбільшим рівнем ризику;
- Професійні інструктори з кібербезпеки разом із CISO організації групують працівників за типами ризику;
- Відповідно до визначених груп і їхніх основних ризиків інструктори формують короткі та інтенсивні тренінги, які згодом проводяться для відповідних аудиторій.

Симуляція фішингових атак

- Створення і розсилка працівникам фішингових мейлів з урахуванням результатів їхнього навчання та виявлених зон ризику в кіберпросторі;
- Ефект несподіванки і особистий досвід суттєво покращують розуміння загроз і негативних наслідків для компанії;
- Реакція працівників на симуляцію фішингової атаки дозволяє спланувати ефективні заходи для боротьби з небезпечною поведінкою: додаткові тренінги, адміністративні заходи тощо.



Комунікаційна підтримка і стимуляція

- Створення і розсилка періодичних інформаційних бюлетенів про успішні кібератаки й інші актуальні події та загрози у сфері кібербезпеки;
- Розсилка текстових, графічних та відео-матеріалів, націлених на асоціативне запам'ятовування інформації та посилення ефекту навчання;
- Виготовлення і доставка поліграфічної та сувенірної продукції для додаткового нагадування про необхідність дотримання правил кібергігієни.

ЦІЛЬОВІ ТРЕНІНГИ З КІБЕРБЕЗПЕКИ

- "Загальні принципи інформаційної безпеки"
- "Соціальна інженерія"
- "Фішинг: атаки через e-mail"
- "Соціальні мережі"
- "Інтернет-браузинг"
- "Безпека мобільних пристроїв"
- "Паролі"
- "Шифрування"
- "Безпека даних"
- "Знищення даних"
- "Безпечний WI-FI"
- "Віддалена робота"
- "Технічна підтримка"
- "Відділ IT"
- "Фізична безпека"
- "Захист персонального комп'ютера"
- "Вас зламано, що тепер?"
- "Advanced Persistent Threat (APT)"
- "Хмарні сервіси"
- "Кроки для забезпечення безпеки"

ЧОМУ ISSP?

- ISSP має єдиний в Україні тренінговий центр із акредитацією від ISC2, EC-Council, Mile2;
- ISSP є стратегічним партнером CybExer в Україні, Грузії, Казахстані та Польщі
- Власна методика ThreatSCALE, визнана провідними технічними університетами світу (MIT, Darthmounth Collegue), галузевими організаціями (SANS Institute) та світовими вендорами (Honeywell);
- Можливість отримати визнані в світі сертифікати міжнародного зразка, такі як Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI) та ін.;
- Авторські навчальні програми, побудовані на основі досвіду лабораторії, SOC та інженерного відділу ISSP;
- Проведення навчальних програм для кіберполіції, МВС, ЦВК та інших державних структур.