Szkolenia w zakresie podnoszenia świadomości zagrożeń w cyberprzestrzeni

Naszym celem, w ramach szkoleń z zakresu *Security Awareness,* jest podniesienie poziomu **świadomości w zakresie zagrożeń oraz sposobów radzenia sobie z nimi** w środowisku pracy, które wykorzystuje urządzenia z dostępem do sieci wewnętrznej przedsiębiorstwa oraz Internetu. Dodatkowo, szkolenia umożliwiają realizację obowiązków nakładanych przez prawo, w tym: Krajowego Systemu Cyberbezpieczeństwa (KSC), RODO czy Krajowej Ramy Interoperacyjności.

Dla kogo

Program szkolenia skierowany jest do każdego odbiorcy, który korzysta na co dzień z urządzeń podłączonych do sieci Internet oraz wewnętrznej sieci LAN organizacji. Udział w szkoleniu jest dostępny dla uczestników **o różnym poziomie zaawansowania technicznego,** ponieważ treść spotkania dostosowujemy do potrzeb i umiejętności pracowników na różnych szczeblach organizacji.

Szczegółowy zakres szkolenia *Cybersecurity Awareness*

Moduł I: Podstawy cyberbezpieczeństwa	
1.1	**Podstawowe pojęcia w zakresie cyberbezpieczeństwa - kontekst globalny.**
1.2	**Każdego da się złamać... czyli ataki socjotechniczne. Teoria i praktyka.**
1.3	**Dlaczego jesteśmy podatni – ludzkie słabości i emocje.**
1.4	**Wybór ofiary ataku oraz mechanika ataku.**
1.5	**Czujność jako podstawa obrony. Przykłady ataków oraz co warto zapamiętać.**
Moduł II: Cyberbezpieczeństwo na co dzień	
2.1	**Jak działamy w sieci i dlaczego to może być niebezpieczne, perspektywa służbowa i prywatna.**
2.2	**Portale społecznościowe – współczesny zasób wiedzy:**
a.	Jakie informacje o sobie przekazujemy na portalach społecznościowych.
b.	OSINT- czyli co „sieć” wie o nas.
c.	Zachowanie czujności, czyli na co zwrócić uwagę prowadząc działania w sieci.
d.	Dobre praktyki w portalach społecznościowych.

2.3	**Pieniądze w sieci - bankowość elektroniczna:**	
	a.	Dzisiejsza rzeczywistość bankowości elektronicznej - perspektywa służbowa i prywatna.
	b.	Tam gdzie są pieniądze, są też przestępcy - metody i ewolucja ataków na użytkowników bankowości elektronicznej wraz z przykładami.
	c.	Czego warto się nauczyć korzystając z bankowości elektronicznej.
	d.	Co jest nie tak z tym bankiem - bezpieczne korzystanie z pieniędzy on-line.
2.4	**Hasła – jak stworzyć hasło łatwe do zapamiętania a trudne do złamania:**	
	a.	Naturalna skłonność do łatwych haseł – dlaczego jej nie ulegać?
	b.	Silne hasła – czyli jakie?
	c.	Dlaczego nie można mieć jednego hasła do wszystkich systemów?
	d.	Zarzadzanie wieloma hasłami - jak sobie z tym poradzić?
	e.	Czy hasła są łamane czy pozyskane?
	f.	Podsumowanie – najważniejsze zasady tworzenia i użytkowania haseł.
2.5	**Bezpieczny komputer:**	
	a.	Backup i przywracanie danych.
	b.	Firewall, antywirus, antyspam.
	c.	Bezpieczne korzystanie z chmury obliczeniowej.
	d.	Aktualizowanie oprogramowania.
	e.	Bezpieczna sieć Wi-Fi w domu, pracy i otoczeniu.
	f.	Lista kontrolna bezpiecznego komputera.

Moduł III: Cyberbezpieczeństwo w firmie		
3.1	**Polityka bezpieczeństwa w firmie – wstęp do zagadnienia:**	
	a.	Budowanie polityki bezpieczeństwa.
	b.	Obowiązek ochrony informacji.
	c.	Zabezpieczenie środowiska pracy.
3.2	**Bezpieczny pracownik i jego dane:**	
	a.	Sporządzanie kopii zapasowych.
	b.	Które pliki archiwizować?
	c.	Oprogramowanie z różnych źródeł.
	d.	Szyfrowanie danych.
	e.	Kopie bezpieczeństwa.
3.3	**Bezpieczeństwo fizyczne sprzętu elektronicznego:**	
	a.	Ochrona przed człowiekiem.
	b.	Ochrona przed przyrodą.
	c.	Zabezpieczenia fizyczne.
3.4	**Bezpieczeństwo w podróży:**	
	a.	Gdzie się podłączyć do sieci?
	b.	Bezpieczne połączenia do sieci firmowej przez niebezpieczny Internet.
	c.	Bezpieczeństwo fizyczne.
	d.	Kontrola i monitoring dostępu.
	e.	Biometria w zabezpieczeniach dostępu.

Szkolenia to pierwszy krok do bezpiecznego IT

Euvic Solutions dostarcza kompleksowe szkolenia **podnoszące świadomość cyberbezpieczeństwa**. Realizujemy je zarówno **online** i **stacjonarnie.** W pełni dostosowujemy program do potrzeb organizacji zarówno z **sektora publicznego,** jak i **prywatnego,** oraz dla zespołów o różnym poziomie zaawansowania. Oferujemy także specjalistyczne szkolenia produktowe, związane z konkretnymi rozwiązaniami technologicznymi.

Skorzystaj z wiedzy naszych ekspertów i stwórz szkolenie idealnie dopasowane do Twoich potrzeb. Porozmawiajmy o szczegółach.

Skontaktuj się z nami

Jesteśmy częścią Grupy Technologicznej EUVIC

Grupa EUVIC to unikatowa koncepcja biznesowa stanowiąca obecnie największy w Europie Środkowo-Wschodniej konglomerat spółek technologicznych. **Grupa jest połączeniem kilkunastu różnych spółek IT** z komplementarną ofertą i bogatym doświadczeniem.

5500 pracowników

6500 projektów

20+ biura EUVIC

Portfolio EUVIC Solutions

Wdrażamy technologie cyfrowe we wszystkich obszarach działalności firmy, tak by pomóc naszym partnerom stworzyć **nową, konkurencyjną strategię, bazującą na najnowszych osiągnięciach branży IT.** Innowacje technologiczne, które wprowadzamy u naszych klientów, całkowicie zmieniają dotychczasowy sposób funkcjonowania firmy.

- Data Center
- Wirtualizacja
- IT Governance
- Cybersecurity
- Rozwiązania Cloud
- Rozwiązania dla biznesu
- Rozwiązania dla edukacji
- Platforma SOLUTIO
- Komunikacja sieciowa
- SAP
- Przemysł 4.0

Euvic Solutions S. A., Al. Jerozolimskie 98, 00-807 Warszawa,
telefon: +48 22 335 44 44, fax: +48 22 335 4445,
NIP: 5213294904, KRS: 0000813557, REGON: 015760481
www.euvic.solutions