Atelier de instruire în domeniul securității cibernetice

DATA: 27 martie 2024, ora: 10:00 – 12:00

Într-o lume digitală în continuă evoluție, amenințările cibernetice devin tot mai sofisticate, iar avocații, ca gestionari ai unor cantități semnificative de date personale și confidențiale, trebuie să fie în mod special conștienți de riscurile asociate și să știe cum să le gestioneze eficient. Acest atelier este conceput să adreseze nevoia de educație și conștientizare în domeniul securității cibernetice pentru profesioniștii din domeniul juridic din Republica Moldova.

Obiectivele principale ale programului sunt:

Conștientizarea importanței securității cibernetice în domeniul juridic și a impactului potențial al incidentelor de securitate: Acest obiectiv vizează sensibilizarea avocaților cu privire la relevanța securității cibernetice în activitatea lor profesională. Participanții vor înțelege amenințările și riscurile cibernetice comune, precum și consecințele potențiale ale incidentelor de securitate asupra clienților, reputației și operațiunilor firmelor de avocatură. Prin evidențierea importanței securității cibernetice, avocații vor fi motivați să acorde prioritate măsurilor de protecție în activitatea lor zilnică.

Înțelegerea și aplicarea bunelor practici pentru protejarea confidențialității și privilegiului avocat-client în era digitală: Acest obiectiv se concentrează pe modalitățile de protejare a datelor sensibile ale clienților în contextul comunicărilor și stocării electronice. Avocații vor învăța despre tehnicile de criptare a datelor și comunicațiilor, gestionarea și stocarea în siguranță a documentelor electronice, precum și despre best practices pentru utilizarea e-mailurilor și a comunicațiilor online. Aceste cunoștințe vor permite avocaților să mențină confidențialitatea și privilegiul avocat-client în mediul digital.

Dobândirea de competențe practice în gestionarea și securizarea comunicațiilor electronice, a dispozitivelor și a rețelelor: Acest obiectiv se axează pe dezvoltarea abilităților practice ale avocaților în domeniul securității cibernetice. Participanții vor învăța cum să configureze și să actualizeze software-ul de securitate, să utilizeze autentificarea multi-factor (MFA), să securizeze rețelele Wi-Fi și accesul de la distanță. Aceste competențe vor permite avocaților să-și protejeze eficient dispozitivele și rețelele, reducând riscul de incidente de securitate.

Dezvoltarea și implementarea politicilor și procedurilor de securitate cibernetică adecvate pentru firmele de avocatură: Acest obiectiv vizează capacitatea avocaților de a dezvolta și implementa politici și proceduri de securitate cibernetică adaptate nevoilor specifice ale firmelor de avocatură. Participanții vor învăța cum să creeze politici eficiente, să instruiască angajații cu privire la protocoalele de securitate și să dezvolte planuri de răspuns la incidente și recuperare în caz de dezastru. Aceste măsuri vor contribui la crearea unei culturi a securității cibernetice în cadrul firmelor de avocatură.

Asigurarea conformității cu reglementările relevante privind protecția datelor: Acest obiectiv se concentrează pe înțelegerea și respectarea reglementărilor privind protecția datelor. Avocații vor învăța despre cerințele specifice ale acestor reglementări, gestionarea consimțământului și a drepturilor persoanelor vizate, precum și despre obligațiile de raportare și notificare în cazul încălcării securității datelor. Aceste cunoștințe vor asigura că firmele de avocatură operează în conformitate cu cadrul legal privind protecția datelor.

Gestionarea eficientă a riscurilor de securitate cibernetică asociate terților și furnizorilor: Acest obiectiv abordează riscurile de securitate cibernetică care pot apărea din relațiile cu terții și furnizorii.

Avocații vor învăța cum să evalueze și să monitorizeze securitatea cibernetică a furnizorilor, să includă clauze contractuale adecvate și să efectueze due diligence și audituri de securitate cibernetică. Aceste măsuri vor ajuta la reducerea riscurilor asociate schimbului de date sensibile cu părți externe.

Scopul acestui program, este de a vă oferi o introducere în noțiunile fundamentale de securitate cibernetică, precum și instrumentele și resursele cheie de care aveți nevoie pentru a asigura un mediu digital securizat. Pe parcursul sesiunii de instruire ne vom axa pe cele mai recente tipuri de amenințări cibernetice, cum să protejați dispozitivele și datele personale în online, precum și să predați mai departe elevilor noțiunile de bază ale securității cibernetice.

FORMATORI:

Natalia Spînu, Director, Institutul European de Studii Politice din Moldova

Natalia Balaban, avocat, Președintele Consiliului Centrului de Instruire a Avocaților

AGENDA

Atelier de instruire în domeniul securității cibernetice

Deschiderea seminarului

- Reprezentant ...

Prezentarea domeniului de securitate cibernetică

- Introducere în Securitatea Cibernetică;
- Rolul și importanța securității cibernetice;

Tendințe cibernetice. Amenințări cibernetice

- Tipuri de amenințări: malware, phishing, Ingineria socială, Ransomware, Atacuri de tip DDos.

Concepte de bază în igiena cibernetică

- Parolele și managementul acestora;
- Actualizări de software și de ce sunt esențiale;
- Backup și importanța acestuia.

GDPR și Legislația Locală privind Protecția Datelor și Securitatea Cibernetică

- Principiile fundamentale ale GDPR
- Aplicabilitatea GDPR în Republica Moldova

Măsuri de Prevenție și Bune Practici

Navigare în siguranță pe internet

- Identificarea site-urilor de încredere

- Folosirea extensiilor de browser pentru securitate

E-mail și comunicare securizată

- Recunoașterea e-mail-urilor de phishing
- Bune practici în trimiterea și primirea de fișiere
- Criptarea comunicațiilor

Securitatea dispozitivelor mobile și Aplicații

- Securizarea dispozitivelor fizice. Setări de bază: PIN, parolă, autentificare biometrică. Măsuri în caz de pierdere sau furt
- Securitatea Aplicațiilor Mobile. Identificarea și evitarea aplicațiilor malicioase. Permisii ale aplicațiilor: ce să accepți și ce să eviți. Autentificare multi-factor și aplicații de gestionare a parolelor
- Setări de bază pentru securitatea smartphone-urilor și tabletelor
- Aplicații recomandate pentru protecție
- Conștientizarea riscurilor legate de Wi-Fi public

Managementul aplicațiilor

- Instalarea aplicațiilor din surse sigure
- Actualizări și permisiuni ale aplicațiilor
- Identificarea aplicațiilor malițioase

Rețelele de Socializare - cum să navighezi în siguranță

- Setări de confidențialitate și securitate
- Riscurile asociate cu partajarea de informații
- Recunoscând și evitând schemele de scamming

Securitatea cardurilor

- Activarea notificărilor pentru tranzacții și limite de tranzacție
- A nu nota PIN-ul pe card sau în proximitatea lui
- Utilizarea corectă a cardurilor pe site-uri web
- Utilizarea autentificării în două etape la efectuarea tranzacțiilor online

Amenințările din Interior (Insider Threats)

- De ce amenințările din interior sunt un risc distinct față de amenințările externe
- Profilul și motivațiile Atacatorilor din Interior
- Diferențe între atacatorii neglijenți, intenționați și inadvertenți
- Principalele motivații: financiare, revanșă, ideologie, curiozitate, eroare umană.

Metode și tehnici de furt de identitate

- Phishing și atacuri de tip "spear phishing"
- Skimming-ul și clonarea cardurilor
- Malware și keyloggers
- Atacuri de inginerie socială

Prevenirea și răspunsul la Furtul de Identitate

- Securizarea informațiilor personale și financiare
- Utilizarea autentificării cu doi factori
- Ce trebuie făcut dacă sunteți victima unui furt de identitate: pași imediați și recuperare.

Sesiune de întrebări si răspunsuri

Concluzii

Sumar al principalelor aspecte abordate în trainingul de securitate cibernetică;