محاضرة بعنوان الامن السيبر اني وتأثيره على بيئة عمل مهنة المحاماة
من إعداد الدكتور بن ناصف مولود -

مقدمة:

يسعدني أن أقف أمامكم اليوم لأتحدث عن موضوع حيوي ومفصلي في عصرنا الحالي ألا وهو: **"العلاقة بين الأمن السيبر اني، وأخلاقيات مهنة المحاماة، وتأثيرها المباشروالعميق على بيئة العمل."** وقد أشارت المادة 2 من قانون 13-07 المؤرخ في 24 ذي الحجة 1434 المو افق ل 29 أكتوبر 2013 يتضمن تنظيم مهنة المحاماة على ان : المحاماة مهنة حرة ومستقلة تعمل على حماية وحفظ حقوق الدفاع وتساهم في تحقيق العدالة واحترام مبدأ سيادة القانون. ونظرا للتطور التكنولوجي والرقمي الحاصل في العالم الحديث وفي ظل التسارع المذهل للتحول الرقمي الذي أثر على كافة جوانب الحياة المهنية والشخصية لذا باتت مهنة المحاماة بطبيعتها التي تعتمد على السرية والثقة والتعامل مع معلومات حساسة للغاية في صميم هذا التحول. ولقد أصبح المحامون اليوم يعتمدون بشكل مكثف على تكنولوجيا الاعلام والاتصال في كل خطوة: من حفظ بيانات الموكلين، والتواصل الآمن، وإدارة القضايا، وحتى إجراءات التقاضي الإلكتروني.

هذا الاعتماد المتزايد يضع الأمن الرقمي، أو ما نسميه "الأمن السيبراني"، ليس فقط كخيار تكنولوجي، بل **كشرط أساسي للممارسة المهنية الأخلاقية والآمنة والمسؤولة.**

ويعرف الأمن السيبراني على انه **مجموعة من الإجراءات والتقنيات والممارسات المصممة لحماية:**

- **الأنظمة الإلكترونية**: مثل أجهزة الكمبيوتر والخوادم.
- **المعلومات الرقمية**: بيانات الموكلين، المستندات القانونية، المراسلات.
- **الشبكات**: شبكات الإنترنت الداخلية والخارجية.
- **الأجهزة**: الهواتف الذكية، الأجهزة اللوحية، أجهزة التخزين المحمولة.
- **حسابات البريد الإلكتروني المهنية**: التي تُعد بوابة رئيسية للكثير من الهجمات.

وذلك من التهديدات المتنوعة والمتطورة مثل:

- **الاختراقات**: الدخول غير المصرح به إلى الأنظمة.
- **الفيروسات والبرامج الضارة**: التي تُتلف البيانات أو تعطل الأنظمة.
- **سرقة البيانات**: الاستيلاء على معلومات حساسة.
- **هجمات الفدية (Ransomware)**: تشفير البيانات والمطالبة بفدية لإعادة الوصول إليها.
- **التصيد الاحتيالي (Phishing)**: محاولات لخداع المستخدمين للحصول على معلوماتهم السرية.

تهدف هذه الإجراءات الى حماية سرية المعلومات ، سلامتها ، توافرها

وفي هذا الصدد نطرح الإشكالية التالية : - **كيف يمكن ان يؤثر الامن السيبراني على اخلاقيات مهنة المحاماة؟**

للإجابة على هذه الإشكالية قمنا بتسطير الخطة التالية :

قسمنا هذه الدراسة الى مبحثين رئيسيين وكل مبحث يندرج تحته مطلبين.

محاضرة بعنوان الامن السيبر اني وتأثيره على بيئة عمل مهنة المحاماة
من إعداد الدكتور بن ناصف مولود -

مقدمة

المبحث الأول : أهمية الامن السيبر اني في أخلاقيات مهنة المحاماة

المطلب الأول : التزامات المحامي في مجال الامن السيبر اني

الفرع الأول : المحامي كحارس رقمي

الفرع الثاني : التزام المحامي بالالمام بالتقنيات الرقمية الحديثة

الفرع الثالث :الحفاظ على الثقة والسمعة المهنية

المطلب الثاني : المسؤولية القانونية المتزايدة

الفرع الأول : المسؤولية التأديبية

الفرع الثاني : المسؤولية المدنية

الفرع الثالث : المسؤولية الجزائية

المبحث الثاني : استراتيجات تعزيز الامن السيبر اني في مكاتب المحاماة

المطلب الأول : التدابير الوقائية

الفرع الأول : التدابير الوقائية التقنية

التدابير الوقائية الخاصة بالعنصر البشري

المطلب الثاني : تطبيقات عملية على التهديدات السيبرانية وتأثيرها المباشر على بيئة العمل القانونية

خاتمة

التوصيات

الملاحق

محاضرة بعنوان الامن السيبراني وتأثيره على بيئة عمل مهنة المحاماة
من إعداد الدكتور بن ناصف مولود -

المبحث الأول :أهمية الامن السيبراني في أخلاقيات مهنة المحاماة

مهنة المحاماة بطبيعتها تتعامل مع معلومات شديدة الحساسية. فهو لا يتعامل فقط مع تفاصيل شخصية أو مالية، بل أيضًا مع استراتيجيات قانونية، وثائق سرية للغاية، ومعلومات قد تؤثر بشكل كبير على حياة الأفراد أو مستقبل الشركات.

ففي العصر الرقمي، أصبحت هذه المعلومات مخزنة ومعالجة رقميًا. هذا التحول يعني أن المحامي لم يعد فقط مؤتمنًا على الأسرار الشفهية أو الورقية، بل أصبح **حارسًا رقميًا للبيانات**. أي ثغرة أمنية يمكن أن ترتب أضرار كارثية ، ومع الاعتماد المتزايد على التكنولوجيا ازداد حجم الهجمات السيبرانية على مختلف القطاعات بما في ذلك القطاع القانوني ويكفي تسريب معلومة حساسة واحدة لالحاق ضرر بالغ بسمعة المحامي او المؤسسة القانونية .

وفي هذا المبحث سنتطرق الى التزامات المحامي في مجال الامن السيبراني [المطلب الأول] بالإضافة الى المسؤولية القانونية عن الاخلال بهذه المبادئ [المطلب الثاني].

المطلب الأول : التزامات المحامي في مجال الامن السيبراني

نقسم هذا المطلب الى ثلاثة فروعة رئيسية :

الفرع الأول : المحامي كحارس رقمي

انطلاقا من نص المادة 47 من دستور أول نوفمبر 2020 الصادر بموجب المرسوم الرئاسي20-442 ، المؤرخ 30-12-2020 ، عدد رقم 82 :"

لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرّية مراسلاته و اتصالاته الخاصة في أي شكل كانت".

لامساس بالحقوق المذكورة في الفقرتين الأولى والثانية الا بأمر معلل من السلطة القضائية.

كما ورد في نص المادة 24 من قانون تنظيم مهنة المحاماة السالف الذكر:

يستفيد المحامي بمناسبة ممارسة مهنته من:

–الحماية التامة للعلاقات ذات الطابع السري القائمة بينه و بين موكليه،

–ضمان سرية ملفاته ومراسلاته،

حيث نصت المادة 07 من القانون 07/18 المؤرخ في 25 رمضان عام 1439 المو افق ل 10 يونيو سنة 2018الذي يتعلق بحماية الأشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصي على انه : ... لايمكن اطلاع الغير على المعطيات ذات الطابع الشخصي الخاضعة للمعالجة إلا من أجل انجاز الغايات المرتبطة مباشرة بمهام المسؤول عن المعالجة والمرسل اليه وبعد الموافقة المسبقة للشخص المعني ."

استنادا الى ما ورد أعلاه من نصوص دستورية وقانونية فإن المحامي مُلزم قانونيًا وأخلاقيًا بحفظ أسرار موكليه. هذا الالتزام، الذي يُعد جوهر العلاقة بين المحامي والموكل، يمتد اليوم ليغطي البيئة الرقمية بالكامل أي اختراق أمني يعرض هذه السرية للخطر – سواء كان بسبب إهمال داخلي أو هجوم سيبراني خارجي – يمكن ان يؤدي الى انتهاك واضح لقواعد السلوك المهني تحت طائلة العقوبات التأديبية قد تصل الى فقدان الاعتماد والشطب من الجدول الكبير للمحامين ، كما نصت المادة 13 فـ2 من القانون المنظم لمهنة المحاماة على مايلي :" **يجب عليه في كل الحالات أن يحافظ على أسرار موكله وأن يكتم السر المهني** "

لاسيما في التعاملات المالية واثناء قيامه بالتسوية المالية للنزاعات التي أوكلت اليه ويجب عليه في هذه الحالة فتح حساب بنكي خاص لهذه التسوية وألزمته بإيداع في هذا الحساب كافة المبالغ المالية الخاصة بهذه العمليات .

لم يعد يكفي أن يحترم المحامي السرية في اللقاءات الشخصية أو الوثائق المادية بل يمتد هذا الاحترام ليضمن أمان كل ملف إلكتروني، وكل رسالة بريدية، وكل محادثة عبر منصات التواصل، وكل بيانات مخزنة على السحابة. هذا مايتطلب تبني إجراءات أمنية صارمة وتشفير للمعلومات الحساسة.

الاستثناء :

- قد تطلب الجهات الأمنية الوصول إلى بيانات الموكلين بحجة مكافحة الجرائم السيبرانية أو الإرهاب. يجب على المحامي مقاومة أي انتهاك لسرية المعلومات ما لم يكن هناك أمر قضائي ملزم أو استدعاء من نقيب المحامين بمناسبة اجراء تحقيق في ملف تأديبي مع مراعاة التوازن بين الأمن العام والخصوصية.

الفرع الثاني : التزام المحامي بالالمام بالتقنيات الرقمية الحديثة

أصبح يُتوقع من المحامي المعاصر الإلمام بالحد الأدنى من المهارات الرقمية الضرورية للممارسة الآمنة. ويشمل هذا :

- التعامل الواعي مع برامج الحماية ومكافحة الفيروسات.
- التأكد من أمان أساليب تخزين البيانات (سواء على الأجهزة أو السحابة).

- التحقق من صحة الروابط والمرفقات في رسائل البريد الإلكتروني لتجنب التصيد الاحتيالي.
- فهم أساسيات التشفير واستخدامه عند الحاجة.

الفرع الثالث :الحفاظ على الثقة والسمعة المهنية

تعتبر الثقة حجر الزاوية وهي أيضا العملة الأساسية في العلاقة بين المحامي وموكله ، كما تعتمد أيضا بشكل كبير على مدى أمان المعلومات الحساسة التي يشاركها الموكل. أي تسرب للبيانات او أي حادث امني يزعزع هذه الثقة يضر بمصلحة المكتب بشيء لا يمكن إصلاحه حتى ولو لم يرتب أي ضرر مباشر، قد يؤدي إلى فقدان الموكلين، وتشويه السمعة المهنية للمكتب، وصعوبة بالغة في جذب عملاء جدد والاحتفاظ بالعملاء الحاليين وتهديم السمعة التي بنيت على مدار سنوات التي قد تنهار في لحظة بسبب حادث سيبراني.

في حال تعرض بيانات الموكلين للاختراق، قد يتعارض الإبلاغ عن الحادث مع رغبة المحامي في حماية سمعته المهنية.

تفرض قوانين مثل (GDPR) النظام **الأوروبي العام لحماية البيانات** في الاتحاد الأوروبي أو (CCPA) **قانون خصوصية المستهلك في كاليفورنيا** إبلاغ الجهات المعنية والموكلين في حالات معينة.

فإن الأخلاقيات تقتضي الشفافية حتى في غياب الالتزام القانوني.

المطلب الثاني : المسؤولية القانونية المتزايدة

في كثير من الدول حول العالم، تُحمَّل المحامي أو المكتب القانوني مسؤولية قانونية مباشرة إذا ثبت وجود تقصير في حماية بيانات الموكلين .

التشريعات الحديثة لحماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا، أو قوانين حماية البيانات المحلية في العديد من البلدان أو قانون حماية خصوصية المستهلك في كاليفورنيا CCPA المذكورة انفا التي تفرض متطلبات صارمة وإجراءات عقابية وغرامات باهظة على الكيانات التي تفشل في تأمين البيانات الحساسة وعليه فان المحامي لم يعد يملك الاعذار بعدم معرفته للتهديدات الرقمية -أي لاعذر بجهل التقنيات الحديثة-

الفرع الأول : المسؤولية التأديبية

يُخضع القانون رقم 13-07 المؤرخ في 08 يوليو 2013 المعدل والمتمم لقانون المحاماة (91-03) المحامي لنظام تأديبي صارم في حال إخلاله بالتزاماته المهنية، بما في ذلك التقصير في حماية بيانات موكله.

فإن المحامي ملزم بالحفاظ على سرية المعلومات المتعلقة بموكله، ويُعد أي إخلال بهذا الالتزام – سواء بالإفشاء المتعمد أو الإهمال في تأمين البيانات الرقمية – مخالفة تأديبية تستوجب العقاب.

كما يخضع المحامي للمساءلة التأديبية أمام المجلس التأديبي التابع لمنظمة المحامين في حال ثبوت التقصير المهني أو الإخلال بواجباته المهنية. وتتراوح العقوبات التأديبية بين الإنذار، التوبيخ، التوقيف المؤقت عن الممارسة لمدة قد تصل إلى سنة مع النفاذ المعجل أو الشطب

النهائي من جدول المحامين في الحالات الخطيرة التي تمس بشرف المهنة أو تسبب ضررًا جسيمًا للموكل.

كما أشارت نص المادة 118 من القانون رقم 07/13 السالف الذكر التي تنص على : "دون الإخلال بالمسؤولية الجزائية والمدنية المنصوص عليها في التشريع المعمول به، يتعرض المحامي عن كل تقصير في التزاماته المهنية أو بمناسبة تأديتها إلى العقوبات التأديبية المنصوص عليها في هذا القانون."

لقد اتخذ مجلس المنظمة عن طريق مجلسها التأديبي العديد من القرارات التأديبية في حق المحامين الذي ارتكبوا أخطاء جسيمة سواء في حق زملائهم او في حق موكليهم او في حق المتقاضيين او تجاه مجلس المنظمة او في حق الجهات القضائية مثلا : تسريب معلومات ذات طابع سري الى جهات أجنبية ومنع نشر ومناقشة المسائل التأديبية في مواقع التواصل الاجتماعي الخاصة بالمحامين وان مجال مناقشتها هو الجمعية العامة وقد أصدر المجلس التأديبي في هذا الصدد عدة قرارات تأديبية لاسيما في السنوات الأخيرة وصلت الى حد الشطب من الجدول الكبير للمحامين وكذا عقوبة التوقيف عن الممارسة المهنية لمدة سنة مع النفاذ المعجل وهذا بعد اجراء تحقيق وسماع اطراف الشكوى على مستوى لجنة أخلاقيات المهنة التي تسهر دوما على المحافظة على الأعراف والتقاليد النبيلة التي تتمتع بها مهنة المحاماة وقد بلغ عدد القرارات التأديبية الى

الفرع الثاني : المسؤولية المدنية

استنادا على نص المادة 124 من القانون المدني فان المسؤولية المدنية للمحامي في حال إخلاله بالتزاماته المهنية المتعلقة بحماية البيانات الرقمية لموكله، وتقوم هذه المسؤولية

بتوافر أركانها الثلاثة: الخطأ (كإهمال المحامي في اتخاذ التدابير الأمنية الكافية لحماية الملفات الرقمية)، والضرر (مثل تسريب معلومات سرية أو فقدان بيانات مهمة)، والعلاقة السببية بينهما.

ويحق للموكل المطالبة بالتعويض عن الأضرار المادية الناجمة عن هذا الإخلال (كالخسائر المالية المباشرة) والأضرار المعنوية (كالضرر الذي يمس سمعة المتقاضي أو انتهاك الخصوصية)، وذلك عبر دعوى تعويض يرفعها المتضرر أمام المحكمة المختصة.

وتجدر الإشارة إلى أن هذه المسؤولية تظل قائمة حتى لو لم يكن الإخلال مقترناً بقصد ضار، إذ يكفي مجرد الإهمال أو التقصير في تطبيق المعايير المهنية المتعارف عليها في مجال الحماية الرقمية، مع إمكانية اشتراك المسؤولية بين المحامي وأي أطراف أخرى ساهمت في حدوث الضرر (كموفري الخدمات السحابية في حال إثبات تقصيرهم).

مثلا تأسيس المحامي في حق نفس المتقاضين [المدعي-المدعى عليه] ولايراعي في ذلك المصالح المتعارضة لأطراف الخصومة قد تؤدي الى تبادل الملفات والمستندات الى نفس اطراف الخصومة .

الفرع الثالث : المسؤولية الجزائية

تتجسد المسؤولية الجزائية للمحامي في القانون الجزائري عند إخلاله بالتزاماته المتعلقة بحماية البيانات الرقمية للموكلين من خلال عدة نصوص قانونية، حيث يُعاقب بموجب المادة 301 من قانون العقوبات على جريمة إفشاء الأسرار المهنية، والتي قد تصل عقوبتها إلى الحبس من شهرين إلى ستة أشهر وغرامة مالية تقدر من 500دج الى 5000دج . كما يُعرض المحامي للمساءلة الجزائية بموجب المادة 394 مكرر الواردة في القسم السابع تحت عنوان

المساس بأنظمة المعالجة الآلية للمعطيات من قانون العقوبات، الخاصة بالوصول غير المصرح به إلى الأنظمة المعلوماتية والتي تصل عقوبتها إلى الحبس من ثلاثة أشهر إلى 3سنوات وغرامة مالية.

وفي حالات أكثر خطورة تتضمن تلفيق أو تزوير المستندات الإلكترونية، تطبق المادة 215 من قانون العقوبات التي تصل عقوبتها إلى الحبس لمدة [5]خمس سنوات.

ويُضاف إلى ذلك المسؤولية بموجب القانون 18-07 لحماية البيانات الشخصية الذي يعاقب على معالجة البيانات بشكل غير مشروع اين خصص لها فصلا كاملا تحت عنوان الاحكام الجزائية .

وتجدر الإشارة إلى أن هذه العقوبات تزداد شدتها إذا نتج عن الجريمة ضرر جسيم أو إذا ارتكبت في ظروف تشديد كاستغلال الصفة المهنية.

المبحث الثاني : استر اتيجات تعزيز الامن السيبر اني في مكاتب المحاماة

لتحصين بيئة العمل القانونية يتطلب تعزيز الامن السيبراني نهجاً شاملا ومتعدد الأوجه، يجمع بين الحلول التقنية ، والتدابير الإدارية ، والوعي البشري وقد سعت العديد من الدول الى توفير تدابير وقائية نراها في [المطلب الأول] سواء على المستوى التقني [التدابير الوقائية التقنية] او فيما تعلق بالعنصر البشري [التدابير الوقائية الخاصة بالعنصر البشري] ، وسنتطرق أيضا الى اهم التطبيقات العملية للهجمات السيبرانية وكيفية التصدي لها في [المطلب الثاني] .

المطلب الأول : التدابير الوقائية

ارتأينا ان نقسم هذه التدابير الى فرعين رئيسين :

الفرع الأول : التدابير الوقائية التقنية:

* استخدام كلمات مرور قوية وفريدة وتغييرها دوريًا، وتجنب استخدام نفس كلمة المرور لخدمات متعددة.

* التحقق بخطوتين (Two-Factor Authentiquassions - 2FA/MFA) لجميع الحسابات المهنية (البريد الإلكتروني، أنظمة إدارة القضايا، إلخ).

* تشفير الملفات والمراسلات الحساسة، خاصة عند إرسالها خارج المكتب أو تخزينها على أجهزة محمولة.

* تجنب استخدام شبكات Wi-Fi عامة غير آمنة للعمل على الإطلاق، أو استخدام شبكة خاصة افتراضية (VPN) إذا كان ذلك ضروريًا.

* التأكد من تحديث البرامج وأنظمة التشغيل بانتظام لتصحيح الثغرات الأمنية المعروفة.

* النسخ الاحتياطي المنتظم والآمن للبيانات، وتخزين النسخ الاحتياطية بشكل منفصل عن الأنظمة الرئيسية.

* استخدام الأجهزة الشخصية لتجنب تسريب البيانات .

* اجراء تقييم شامل للمخاطر لتحديد نقاط الضعف المحتملة لأنظمة المكتب وبياناته ويساعد هذا التقييم في تحديد الأولويات وتخصيص الموارد بشكل فعال .

الفرع الثاني : التدابير الوقائية الخاصة بالعنصر البشري

* تدريب الموظفين ورفع مستوى الوعي : يعد العنصر البشري اضعف حلقة في سلسلة الامن السيبراني يجب تدريب جميع الموظفين بانتظام بالتعرف على هجمات التصيد الاحتيالي وكيفة التعامل مع المعلومات السرية وكيفية الإبلاغ عن أي نشاط مشبوه .

* التوعية المستمرة بأساليب الاحتيال الإلكتروني الأكثر شيوعاً مثل التصيد الاحتيالي (Phishing) ورسائل البريد الإلكتروني المخادعة.

* وضع سياسة أمن معلومات مكتوبة وواضحة وملزمة لجميع العاملين في المكتب، تحدد الإجراءات المتبعة في التعامل مع البيانات والأنظمة.

* إجراء اختبارات محاكاة لهجمات التصيد الاحتيالي بشكل دوري لتقييم وعي الموظفين وتعزيزه.

*التعاون مع مختصين في الأمن السيبراني .

* إجراء اختبارات اختراق (Penetration Testing) وتقييمات أمان دورية للأنظمة والشبكات للكشف عن الثغرات قبل استغلالها.

* مراجعة صلاحيات الوصول إلى البيانات والأنظمة بانتظام، والتأكد من أن كل موظف لديه فقط الصلاحيات الضرورية لأداء مهامه (مبدأ أقل الامتيازات).

* مراقبة مستمرة لسجلات الدخول إلى الخوادم والأنظمة للكشف عن أي نشاط مشبوه.

* وضع خطة استجابة للحوادث السيبرانية تحدد الخطوات الواجب اتخاذها فور وقوع أي اختراق لتقليل الأضرار والتعافي السريع.

المطلب الثاني : تطبيقات عملية على التهديدات السيبرانية وتأثيرها المباشر على بيئة العمل القانونية

لننظر إلى بعض السيناريوهات الواقعية التي توضح كيف يمكن للتهديدات السيبرانية أن تؤثر بشكل مباشر على مكاتب المحاماة:

الحالة/السيناريو	نوع الهجوم	التأثير المباشر على بيئة العمل المهنية	الدرس المستفاد للمحامي ولمكتبه
سرقة جهاز لابتوب يحتوي ملفات قضايا حساسة من سيارة المحامي أو من المنزل	فقدان جهاز مادي مع الكشف عن معلومات حساسة.	-**فقدان البيانات**: ضياع وثائق مهمة قد لا يكون لها نسخ احتياطية. - **تسرب معلومات**: وصول معلومات الموكلين السرية إلى أيدي غير مصرح لها. - **مسؤولية قانونية**: قد يواجه المحامي دعوى قضائية من الموكلين لخرق مبدأ السرية. - **تعطيل العمل**: توقف العمل على القضايا المتأثرة حتى استعادة البيانات أو إعادة إنشاء الملفات.	تشفير الأجهزة بالكامل (Full Disk Encryption)، تخزين النسخ الاحتياطية للبيانات بشكل منتظم وآمن (على السحابة أو خوادم المكتب)، واستخدام أدوات المسح عن بعد.

الحالة/السيناريو	نوع الهجوم	التأثير المباشر على بيئة العمل المهنية	الدرس المستفاد للمحامي ولمكتبه
- فتح بريد إلكتروني مزيف يبدو وكأنه من المحكمة أو من موكل معروف، ويحتوي رابطًا خبيثًا.	- تصيّد احتيالي (Phishing) يؤدي إلى تسريب بيانات دخول أو برامج ضارة.	-- **تسريب بيانات دخول:** قد يؤدي إلى اختراق حساب البريد الإلكتروني للمحامي أو نظام إدارة القضايا. -**اختراق شامل:** إذا كانت بيانات الدخول تسمح بالوصول إلى شبكة المكتب، فقد يؤدي ذلك إلى هجوم فدية أو سرقة بيانات على نطاق واسع. -**فقدان الثقة:** الموكلون سيفقدون الثقة إذا تم تسريب معلوماتهم عبر بريد إلكتروني خاص بالمحامي.	توعية الموظفين والزملاء بالتحقق الدقيق من هوية المرسل، عدم النقر على الروابط المشبوهة، والإبلاغ عن رسائل البريد الإلكتروني المريبة. **تفعيل التحقق بخطوتين.**

الحالة/السيناريو	نوع الهجوم	التأثير المباشر على بيئة العمل المهنية	الدرس المستفاد للمحامي ولمكتبه
اختراق شبكة المكتب عبر ثغرة في برنامج قديم أو جهاز غير محدث.	**هجوم فدية** يشفر جميع الملفات على الشبكة ويطالب بفدية.	- تعطيل كامل للعمل: المحامون لا يستطيعون الوصول إلى أي ملفات، أنظمة البريد الإلكتروني، أو قواعد البيانات. - خسائر مالية ضخمة: دفع الفدية (إذا تم اختيار ذلك)، تكاليف استعادة الأنظمة، وتكاليف الفرص الضائعة بسبب توقف العمل. مسؤولية قانونية: قد يتم مقاضاة المكتب لعدم حماية بيانات الموكلين بشكل كافٍ. ضرر بالسمعة: إعلان الاختراق يضر بسمعة المكتب بشدة.	أهمية جدران الحماية القوية التحديث المنتظم لجميع البرامج والأنظمة، النسخ الاحتياطية المتكررة والمنفصلة للبيانات، ووجود خطة استجابة سريعة للتعافي من الهجمات.

الحالة/السيناريو	نوع الهجوم	التأثير المباشر على بيئة العمل المهنية	الدرس المستفاد للمحامي ولمكتبه
تعرض هاتف محامي للسرقة أو الضياع وهو يحتوي على معلومات تخص قضايا جارية.	**فقدان جهاز محمول مع إمكانية الوصول إلى معلومات حساسة.**	**كشف معلومات سرية:** إذا لم يكن الجهاز مؤمناً بشكل كافٍ. **فقدان بيانات:** ضياع محادثات، ملاحظات، أو وثائق. **تعطيل الاتصال:** فقدان القدرة على التواصل الفوري مع الموكلين أو الزملاء.	**تشفير الأجهزة المحمولة،** استخدام كلمات مرور قوية أو بصمة الإصبع/الوجه للفتح، وتفعيل خاصية المسح عن بعد(Remote Wipe). تجنب تخزين معلومات حساسة جداً على الأجهزة الشخصية.

خاتمة

في ظل عالم رقمي سريع التغيّر ومحاط بالتهديدات، أصبح من الضروري والملح على كل محامٍ ومكتب محاماة أن يدرك أن **الأمن السيبراني ليس مجرد رفاهية تقنية، بل هو جزء لا يتجزأ من أخلاقيات المهنة، ومسؤولية قانونية، وضمانة لاستمرارية العمل.**

إن بناء ثقافة أمنية قوية داخل مكاتبنا ومحيطنا المهني، من خلال التعليم المستمر، وتطبيق الإجراءات الوقائية، والاستعانة بالخبرات المتخصصة، لم يعد خياراً، بل هو **استثمار ضروري** في مستقبل مهنة المحاماة وسلامة موكلينا.

دعونا نتذكر دائمًا هذه المقولة:

"احترام سرية الموكل لا يكتمل إلا باحترام خصوصيته الرقمية."

وإن النجاح في هذا العصر الرقمي يعتمد بشكل كبير على قدرتنا على التكيف، والتعلم، وحماية ما هو ثمين، ألا وهي ثقة الموكلين وسلامة معلوماتهم.

استنادا الى ماتم التطرق اليه اقدم بين ايديكم جملة من التوصيات نراها ضرورية لتدعيم مهنة المحاماة وحماية بيانتهم من الهجمات والاختراقات السيبرانية التي يمكن ان يتعرض لها المحامون ومكاتبهم وهي كالاتي :

- ضرورة تعديل القانون المنظم لمهنة المحاماة 07/13 تماشيا مع دستور اول نوفمبر 2020 لاسيما المواد 39و56و169 و170 وكذا تماشيا مع قانون07/18 **الذي يتعلق بحماية الأشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصي.**
- الزامية اجراء ورشات تكوينية تنصب حول موضوع الامن السيبراني وحماية المعطيات.

- استحداث مقياس الامن السيبراني وانعكاساته على اخلاقيات المهنة يدرس لطلبة الكفاءة المهنية للمحاماة .
- استحداث لجان تقنية مختصة في مجال الامن السيبراني على مستوى منظمات المحامين تحت اشراف السيد النقيب لتقديم الدعم الفني والتقني و القانوني لمكاتب المحاماة والأفراد، وضمان الامتثال للقوانين، لمواجهة التهديدات الإلكترونية التي تستهدف المهنة.

أشكركم على حسن استماعكم، و أتطلع إلى مناقشة أي أسئلة قد تكون لديكم.

الملاحق