

قوانين الحماية من الاحتيال والاختراق الرقمي للبيانات

Data Fraud and Hacking Protection Laws



الأستاذ الدكتور

منال البلقاسي

أستاذ نظم المعلومات المساعد

ووكيل الجودة وخدمة المجتمع معهد الإدارة كفر الشيخ

كاتبة في المعلوماتية والذكاء الاصطناعي

الطبعة الأولى

٢٠٢٥



دار الأمل

للشؤون الإدارية والإعلامية

٠١٢٨١٠٠٠٠٠٣

قوانين الحماية من الاحتيال والاختراق الرقمي للبيانات

Data Fraud and Hacking Protection Laws

الأستاذ الدكتور

منال البلقاسي

أستاذ نظم المعلومات المساعد

ووكيل الجودة وخدمة المجتمع معهد الإدارة كفر الشيخ

كاتبة في المعلوماتية والذكاء الاصطناعي

الطبعة الأولى

٢٠٢٥

الناشر

دار الأهرام للإصدارات القانونية

٠١٢٨١٠٠٠٠٠٣

الطبعة : ٢٠٢٥

رقم الإيداع : ١٦٦٥-٢٠٢٤

الترقيم الدولي : ١-٦-٨٦٤٣٢-٩٧٧-٩٧٨

الناشر : دار الأهرام للإصدارات القانونية

٦٦ ش قناة السويس - المنصورة

٠١٢٨١٠٠٠٠٠٣

جميع الحقوق محفوظة للناشر

ولا يجوز نشر أي جزء من هذا الكتاب أو اختزان مادته بطريقة الاسترجاع
أو نقله على أي نحو أو بأية طريقة سواء كانت إلكترونية أو ميكانيكية
أو خلاف ذلك إلا بموافقة الناشر على هذا كتابة ومقدماتاً

فهرس المحتويات

الفصل الأول

قوانين حماية البيانات والاتصالات (COPPA)

- مصطلحات قانون مكافحة الجرائم الإلكترونية..... ١٤
- قانون الاتصالات (Communications Act) في المملكة المتحدة ١٥
- قانون الحماية من التحرش (Protection from Harassment Act)..... ١٦
- تطبيقات قانون الحماية من التحرش والتقليل منه
- (Protection from Harassment Act) ١٧
- قانون مكافحة الجرائم الإلكترونية (Canadian Anti-Spam Legislation) ١٧
- اجراءات تفعيل قانون مكافحة الجرائم الإلكترونية في كندا- (Canadian Anti-Spam Legislation) ١٨
- اللائحة العامة لحماية البيانات (General Data Protection Regulation) ٢٠
- حقوق اللائحة العامة لحماية بيانات (GDPR) الافراد ٢٢
- تنظيم الإبلاغ عن الانتهاكات..... ٢٣
- قانون جرائم الاتصالات الإلكترونية (Electronic Communications Act) .. ٢٥
- قانون القرصنة (Copyright Act) ٢٦
- قانون الجرائم المعلوماتية (Criminal Code Act) ٢٧
- قانون الخصوصية والبيانات الشخصية (Privacy Act) ٢٨
- قوانين الاتحاد والولايات الفردية..... ٢٩
- قانون الأمان الإلكتروني والخصوصية (Privacy Act) ٢٩

الفصل الثاني

اختراق البيانات والثغرات الأمنية

- تعريف الاختراق..... ٣٤
- أهمية الاختراق..... ٣٤

- ٣٥.....اهداف الاختراق
- ٣٦.....مصطلحات الاختراق
- ٣٧.....الثغرة (Vulnerability)
- ٣٨.....اختبار الاختراق (Penetration Testing)
- ٣٩.....جمع المعلومات (Reconnaissance)
- ٤٠.....فحص الشبكة (Network Scanning)
- ٤١.....اكتشاف الشبكة (Network Discovery)
- ٤٢.....المسح السلكي (Wired Scanning)
- ٤٣.....المسح اللاسلكي (Wireless Scanning)
- ٤٤.....اكتشاف الجهاز (Host Discovery)
- ٤٤.....بث الطلبات (Probe Broadcasting)
- ٤٨.....البث (Broadcasting)
- ٤٩.....الطلب (Request)
- ٥٠.....الاستجابة (Response)
- ٥٠.....الاختيار (Selection)
- ٥١.....الاستجابة للطلبات (Response to Probes)

الفصل الثالث

قوانين الاحتيال الإلكتروني (Cyber Fraud)

- ٦٥.....الاحتيال الإلكتروني (Cyber Fraud)
- ٦٦.....الاحتيال المالي
- ٦٧.....الاحتيال بالهوية
- ٦٨.....فتح حسابات مالية
- ٦٨.....استخدام معلومات الهوية المسروقة
- ٦٩.....تقديم الطلب
- ٧١.....التسويق الإلكتروني

- الاحتيال بتسجيل العقارات..... ٧٢.....
- التقديم على القروض والائتمان..... ٧٣.....
- الاحتيال ببطاقات الائتمان ٧٥.....
- الاحتيال عبر البريد الإلكتروني..... ٧٦.....
- الاضطهاد النصي Phishing ٧٧.....
- الاحتيال بالعروض الوهمية..... ٨٠.....
- الاحتيال بالتمويل الجماعي..... ٨١.....
- الاحتيال بالتسويق الإلكتروني..... ٨١.....
- الاحتيال بالمعلومات الشخصية..... ٨٣.....
- الاحتيال بالعملات الرقمية..... ٨٤.....

الفصل الرابع

الخدمات البينية (Intermediary Services)

- خدمة توزيع الأمان (Security Distribution Service) ٨٨.....
- خدمة الوساطة البرمجية (Middleware Service) ٨٩.....
- خدمة التخزين المؤقت (Caching Service) ٩٠.....
- خدمة التحويل (Proxy Service) ٩١.....
- خدمة الشحن (Shipping Service) ٩٢.....
- الخدمات التطبيقية (Application Services) ٩٣.....
- الخدمات المتوفرة بروتوكولاً (Protocol-based Services) ٩٤.....
- استجابة استكشاف الشبكة (Network Discovery Response) ٩٥.....
- استجابة فحص الأمان (Security Scan Response) ٩٦.....
- استجابة طلب الخدمة (Service Request Response) ٩٧.....
- استجابة عملية التحقق (Authentication Response) ٩٨.....
- تسجيل المعلومات (Logging Information) لأغراض التوثيق والتحليل..... ١٠٠.....
- تحديد العلاقات (Relationship Identification) بين الأجهزة المكتشفة..... ١٠٢.....
- الاستطلاع المباشر (Direct Observation) للمراقبة ١٠٨.....

الفصل الخامس

اختبار الثغرات الأمنية (Exploitation)

- تطبيق الهجمات..... ١١٥
- الوصول غير المصرح ١١٦
- الجدر النارية (Firewall) ١١٧
- مصطلحات في الثغرات الامنية..... ١١٨
- وسائل تقييم وتصحيح الثغرات..... ١٢٠
- البرامج الخبيثة (Malware) ١٢١
- تصيد الهوية (Phishing) ١٢٢
- تحليل سلوك الشبكة (Network Behavior Analysis) ١٢٣
- التشفير (Encryption) ١٢٣
- الاعتراف بالحقوق (Authorization) للتحقق من صلاحيات الوصول للبيانات. ١٢٤
- التوقيع الرقمي (Digital Signature) للتأكد من هوية المرسل وسلامة
- البيانات..... ١٢٥

الفصل السادس

اختراقات بيانات الهواتف الذكية

- تقنيات تعقب الهواتف المحمولة..... ١٢٩
- نظم تحديد المواقع العالمية (GPS) ١٣٠
- الشبكات الخلوية..... ١٣١
- تقنيات البلوتوث (Bluetooth) ١٣٢
- تقنيات الواي فاي (Wi-Fi) ١٣٣
- تقنيات تعقب البيانات الخلفية (Back-end Data Tracking) ١٣٤
- الاختراق الأخلاقي (Ethical Hacking) ١٣٦
- المصطلحات الشائعة للاختراق الأخلاقي..... ١٣٦

- تقنيات تعقب البيانات الجغرافية (Geofencing)..... ١٣٧
- الاختراق أخلاقي (Ethical Hacking) ١٣٨
- اختراق غير الأخلاقي (Unethical Hacking)..... ١٣٩
- العواقب القانونية للاختراق غير الأخلاقي..... ١٤٠
- التشريعات المحلية للاختراق الأخلاقي..... ١٤٢
- الثغرات الأمنية (Security Vulnerability) ١٤٣
- اسباب الثغرات الامنية..... ١٤٣
- آليات معالجة الثغرات الأمنية في الأنظمة والتطبيقات..... ١٤٤
- استراتيجيات التعامل مع الاختراق غير الأخلاقي للثغرات الأمنية..... ١٤٥
- تطبيقات الاختراقات غير الاخلاقية..... ١٤٧
- تطبيقات الهجوم الأخلاقي ١٤٨
- أهداف تطبيقات الاختراق غير الأخلاقية ١٤٩
- القرصنة الإلكترونية (Cybercrime) ١٤٩
- الاختراق السيبراني (Hacking) ١٥٠

الفصل السابع

الاعتداء الرقمي والتنمر الإلكتروني (Cyberbullying)

- الاعتداء الرقمي (Cyberbullying) ١٥٥
- اسباب الاعتداء الرقمي (Cyberbullying) ١٥٧
- اهداف الاعتداء الرقمي (Cyberbullying) ١٥٨
- رعاه الاعتداء الرقمي (Cyberbullying) ١٥٨
- انواع الاعتداء الرقمي (Cyberbullying) ١٥٩
- التنمر الإلكتروني (Cyberbullying) ١٦٠
- آثار التنمر الإلكتروني على الضحية..... ١٦١
- مكافحة التنمر الإلكتروني..... ١٦٢
- التشهير الرقمي (Cyber defamation) ١٦٤

- اسباب التشهير الرقمي ١٦٥
- اهداف التشهير الرقمي ١٦٦
- اليات التشهير الرقمي (Cyber defamation) ١٦٧
- استراتيجيات مواجهة التشهير الرقمي (Cyber defamation) ١٧٠
- تحديد المعلومات الكاذبة ١٧٢
- التواصل مع المنصات الرقمية ١٧٢
- المضايقات الإلكترونية (Cyberstalking) ١٧٥
- التحرش الإلكتروني ١٧٥
- اسباب التحرش الإلكتروني ١٧٦
- مصادر التحرش الإلكتروني ١٧٧
- أنشطة التحرش الإلكتروني ١٧٧
- اضرار المضايقة والتحرش الإلكتروني ١٧٨
- اليات مواجهة المضايقة والتحرش الإلكتروني ١٨١
- تشريعات وقوانين مواجهة المضايقة والتحرش الإلكتروني ١٨٢

الفصل الثامن

الانتحال والتميز للهويات الرقمية (Catfishing)

- انتحال الهوية الرقمية ١٨٧
- أسباب انتحال الهوية الرقمية ١٨٨
- أهداف انتحال الهوية الرقمية ١٨٨
- اضرار ونتائج انتحال الهوية الرقمية ١٨٩
- اليات مواجهة ومكافحة انتحال الهوية الرقمية ١٩٠
- التحريض الرقمي (Cyber incitement) ١٩١
- التمييز الرقمي (Cyber discrimination) ١٩١
- تعريف التمييز الرقمي (Cyber discrimination) ١٩٢
- أسباب التمييز الرقمي ١٩٣
- أهداف التمييز الرقمي ١٩٣

- اضرار التمييز الرقمي ١٩٤
- مكافحة التمييز الرقمي والحد من أضراره ١٩٥
- التجسس الرقمي (Cyber espionage) ١٩٦
- تعريف التجسس الرقمي (Cyber espionage) ١٩٧
- أنواع التجسس الرقمي ١٩٧
- أهداف التجسس الرقمي ١٩٨
- اضرار التجسس الرقمي على الفرد والمجتمع ١٩٩
- معالجات التجسس الرقمي ٢٠٠

الفصل التاسع

قوانين الحوسبة السحابية الضبابية (Fog Computing)

- الحوسبة الضبابية (Fog Computing) ٢٠٤
- التهديدات المتقدمة والمستمرة (Advanced Persistent Threats - APTs) ٢٠٦
- البيانات الضخمة (Big Data) ٢٠٧
- الذكاء الصناعي (Artificial Intelligence - AI) ٢٠٧
- الحوسبة اللامركزية (Decentralized Computing) ٢٠٨
- التعلم الآلي (Machine Learning) ٢٠٩
- الشبكات الاجتماعية (Social Networks) ٢١٠
- المدفوعات الرقمية (Digital Payments) ٢١١
- عمليات الأتمتة (Automation) ٢١٢
- الحوسبة الحافة (Edge Computing) ٢١٣
- الواقع المعزز (Augmented Reality - AR) ٢١٤
- الواقع الافتراضي (Virtual Reality - VR) ٢١٥
- التوثيق الثنائي (Two-Factor Authentication - ٢FA) ٢١٦
- الاعتراض (Interception) ٢١٧
- التطبيقات النصية الضارة (Malicious Scripts) ٢١٨
- المصادقة الثنائية (Biometric Authentication) ٢١٩

- البرامج الضارة المتقدمة (Advanced Persistent Threats - APTs) ٢٢٠
- التحكم الأبوي (Parental Control) ٢٢١
- البرامج الضارة المتقدمة (Advanced Persistent Threats - APTs) ٢٢٢
- التخزين السحابي: (Cloud Storage) ٢٢٣
- التصيد الاحتيالي Phishing ٢٢٤
- القرصنة (Hacking) ٢٢٥
- تقنيات تعقب الهواتف المحمولة ٢٢٦

قائمة المراجع : ص ٢٢٩