تُعرّف القرصنة الإلكترونية باستغلال ثغرات أنظمة الكمبيوتر والشبكات، من قِبل فرد أو أكثر، بهدف الوصول غير القانوني إلى معلومات محمية، مُعاقباً عليها قانونياً. بدأت هذه الظاهرة انتشارها في التسعينيات عبر منصات مثل نابستر. تستخدم أساليب متنوعة كالهندسة الاجتماعية (التلاعب بالبشر)، وقرصنة كلمات المرور (التجربة والخطأ، هجمات القواميس)، وإصابة الأجهزة ببرامج ضارة، واستغلال شبكات لاسلكية غير آمنة، واكتساب الوصول إلى "الأبواب الخلفية"، والتجسس على البريد الإلكتروني، وتسجيل ضغطات المفاتيح، وإنشاء أجهزة كمبيوتر "زومبي". تُشكّل القرصنة تهديدًا للخصوصية، وتعطيل الأنظمة، والابتزاز المالي، وسرقة البيانات، وبيع المعلومات. الابتزاز الإلكتروني، جريمة رقمية متنامية، يُهدد فيها المُبتز الضحية بنشر معلومات خاصة أو صور مقابل منفعة. تنوعت أنواعه: عاطفي (استغلال العلاقات)، مالي (سرقة بيانات مالية)، مؤسسي (استهداف الشركات)، تشهيراتي (نشر معلومات مسيئة)، رقمي عام (برامج الفدية). تختلف ضحايا الابتزاز، فتشمل شخصيات اعتبارية، أطفالاً، ونساءً. يعاقب القانون المصري الابتزاز بالسجن لمدة لا تقل عن ستة أشهر. أبرزت بعض الحوادث المأساوية في مصر والعالم العربي خطورة هذه الجريمة. يُحرم الإسلام الابتزاز، باعتباره إشاعةً للفاحشة، وانتهاكاً للضروريات الخمس (الدين، النفس، العرض، العقل، المال). يُعتبر أخذ الأموال بالابتزاز أكلاً لأموال الناس بالباطل. للابتزاز آثار نفسية واجتماعية سلبية، كشعور انعدام الأمن، فقدان الثقة بالنفس، الاكتئاب، الاحتراق النفسي، ومحاولات الانتحار. لحماية النفس، يُنصح باستخدام كلمات مرور قوية ومصادقة متعددة العوامل، والحذر من التصيد الاحتيالي، وإدارة البصمة الرقمية، والحفاظ على تحديث الأجهزة، وتجنب المواقع المشبوهة، وإيقاف تشغيل الميزات غير الضرورية، وتجنب استخدام شبكات الواي فاي العامة دون VPN، واستخدام برنامج مكافحة فيروسات جيد.