يُعتبر قطاع التعليم العالي هدفًا رئيسيًا للهجمات الإلكترونية نظرًا لاحتواء أبحاثه على بيانات قيّمة، وسهولة اختراقه بسبب كثرة المستخدمين ونقاط الدخول. وقد شهد عام 2022 زيادة كبيرة في هذه الهجمات، مع ارتفاع بنسبة 110% في هجمات برمجيات خبيثة لإنترنت الأشياء و 51% في هجمات الفدية في النصف الأول من العام، حسب بيانات SonicWall. لذا، يجب على المؤسسات التعليمية اتخاذ خطوات لحماية نفسها، بدءًا بتبني عقلية أمنية قائمة على مراقبة الشبكة وحراسة المحيط الخارجي لمنع الوصول غير المصرح به. يجب تطبيق مبدأ "انعدام الثقة" مع المصادقة المستمرة، وتدريب المستخدمين على سياسات قوية لكلمات المرور والمصادقة متعددة العوامل، وتعريفهم بعلامات الهجمات مثل BEC (اختراق البريد الإلكتروني للأعمال)، والتي تُعتبر الأكثر تكلفة. كما يتطلب الأمر تأمين شبكات الواي فاي بخدمات تصفية المحتوى، ومراقبة الشبكة باستمرار، وتجزئتها لمنع انتشار الهجمات. وأخيرًا، يعد إعداد خطة للاستجابة للحوادث والتعافي من الكوارث أمرًا بالغ الأهمية، بما في ذلك نسخ البيانات الاحتياطية وإعلام المستخدمين بإجراءات الطوارئ. فالتخطيط الجيد يُحسّن فرص مواجهة مجرمي الإنترنت.