PRIVAL

Enquête sur les cyberattaques dans l'éducation britannique 2025

Points clés

Contexte

L'enquête sur les atteintes à la **cybersécurité de 2025** offre un aperçu détaillé de la capacité des établissements éducatifs britanniques à faire face à **l'augmentation des menaces numériques**. Le rapport évalue **l'organisation**, les **ressources** et la **culture cyber** de ces institutions, en soulignant les écarts de maturité et leur capacité à adapter rapidement leurs pratiques.

La majorité des établissements sondés montre des progrès notables en gouvernance et sensibilisation à la cybersécurité, avec des stratégies plus claires et un engagement croissant des directions.

Cependant, les plus **petits établissements** ou ceux à **budget limité** ont du mal à suivre l'évolution des attaques et à renforcer leur résilience numérique.

Les établissements éducatifs **surpassent le secteur privé** grâce à l'**engagement des responsables** et à la **prise de conscience** de l'importance de **sécuriser l'enseignement** et les **systèmes critiques**. La gestion du changement, la pénurie de compétences et la pression sur les ressources restent des **défis majeurs** pour une partie du secteur.

Institutions concernées

Écoles primaires : L'enquête a interrogé 250 écoles, souvent marquées par une gouvernance changeante et des ressources informatiques limitées. Ces établissements fonctionnent avec de petites équipes TI, externalisent souvent leurs services numériques, et ont un besoin urgent de sensibilisation des enseignants et élèves.

Écoles secondaires : Parmi les 240 écoles incluses, on note une maturité numérique plus élevée. Elles gèrent plus d'utilisateurs, des systèmes informatiques plus complexes et investissent davantage dans la formation et la gestion des risques. Cependant, la diversité des outils numériques et la rotation des équipes compliquent la gestion des accès et des usages.

Collèges d'enseignement supérieur : Les 52 collèges étudiés se distinguent par des environnements ouverts, une forte population adulte et une gestion efficace des ressources pédagogiques et numériques. Ils adoptent des politiques de gouvernance avancées et gèrent rapidement les incidents cyber.

Universités : Parmi les 32 universités, la cybersécurité est bien intégrée grâce à des équipes dédiées, des politiques claires, des audits réguliers et une solide protection des données. Malgré des technologies avancées, la recherche et les collaborations internationales exposent ces institutions à des menaces, exigeant une gestion stratégique.

Les établissements éducatifs évoluent dans des contextes variés, influencés par leur taille, leurs utilisateurs et la criticité des données. Ils restent des cibles fréquentes de cyberattaques, révélant leur vulnérabilité numérique. Un accompagnement personnalisé et le partage de bonnes pratiques sont essentiels pour renforcer leur cybersécurité.

Une menace omniprésente
du primaire à l'université

Les établissements éducatifs sont particulièrement ciblés par les cyberattaques, illustrant leur vulnérabilité persistante au sein de l'écosystème numérique national.

- **Universités :** 91 % ont signalé au moins une cyberattaque au cours des 12 derniers mois. Ce taux exceptionnellement élevé reflète l'attractivité de ces institutions pour les cybercriminels, en raison de la valeur des données universitaires et de la forte exposition internationale.

- **Collèges :** 85 % ont été touchés, soulignant à la fois leur rôle de passerelle vers l'enseignement supérieur et leur gestion accrue de données sensibles concernant les étudiants et le personnel.

- **Écoles secondaires** : 60 % ont subi des attaques, un chiffre conséquent qui révèle que même les structures de taille intermédiaire restent au cœur de la cible des cybermenaces.

- **Écoles primaires :** 44 % déclarent au moins un incident, ce qui, bien que moins élevé, pointe une exposition croissante des établissements accueillant les plus jeunes élèves, souvent dotés de ressources TI moins sophistiquées.

L'omniprésence des cyberattaques montre que la menace n'épargne aucune catégorie d'établissement, du primaire à l'université. Plus la structure gère de **systèmes complexes** et de **données à forte valeur**, plus elle attire **l'intérêt des attaquants**.

Types d'attaques Identifiées

Phishing : Quasi universel (89 à 97 % selon le type d'établissement). Le phishing reste la menace la plus courante, exploitant la vulnérabilité humaine à travers des courriels trompeurs ou des liens malveillants. Les établissements scolaires, où l'usage du courrier électronique est massif, sont particulièrement exposés, rendant la sensibilisation essentielle à tous les échelons.

Vol d'identité : 32 % (écoles primaires) à 68 % (collèges et universités). Les attaques par vol d'identité ciblent la crédibilité des établissements, en permettant à des cybercriminels de se faire passer pour des membres du personnel ou des étudiants. Cela peut entraîner la diffusion d'informations frauduleuses, la compromission de communications internes et l'accès indu à des ressources protégées.

Logiciels malveillants : Fréquence plus élevée dans l'enseignement supérieur (42 %). Les universités et collèges, riches en données et travaillant souvent avec des partenaires externes, subissent davantage d'infections par logiciels malveillants. Ces logiciels malveillants perturbent les systèmes, peuvent chiffrer des fichiers critiques (ransomware) ou exfiltrer des données sensibles, impactant la continuité pédagogique et la réputation institutionnelle.

Attaques par déni de service : Jusqu'à 36 % des collèges et universités. Les attaques DDoS (déni de service distribué) saturent les infrastructures numériques, rendant les plateformes e-learning ou administratives inaccessibles. Ce type d'attaque génère des interruptions de service, ralentit les opérations courantes et fragilise la confiance des utilisateurs, étudiants comme personnel.

Priorités stratégiques
pour les établissements éducatifs

La cybersécurité est désormais une nécessité pour les établissements éducatifs. Cela passe par des actions concrètes : chartes, codes de conduite numériques et budgets dédiés pour prévenir les risques. Une communication claire avec élèves, enseignants et parties prenantes renforce la confiance et une culture de vigilance partagée.

1. Collèges et universités

Ces établissements se démarquent par des outils avancés, des stratégies structurées et des investissements significatifs. Centres de réponse aux incidents, audits réguliers et budgets dédiés sont des atouts majeurs.

2. Écoles primaires et secondaires

Ces écoles progressent grâce à des chartes numériques et des sauvegardes cloud. Cependant, des lacunes subsistent : manque de ressources TI spécialisées et gestion réactive des mises à jour.

Meilleures pratiques observées :

Responsables dédiés (CISO ou référent SSI) : Présents dans plus de 80 % des établissements, ils coordonnent la stratégie cybersécurité, gèrent les incidents et veillent à la sensibilisation continue.

Politiques et formations : Procédures claires, simulation d'incidents, et sensibilisation régulière permettent une meilleure anticipation et réaction.

Collaboration sectorielle : Partage d'informations et mutualisation des ressources avec d'autres établissements favorisent une amélioration collective.

Renforcer
la Résilience

Sophistication croissante des cybermenaces : Les cyberattaques deviennent de plus en plus complexes, exploitant les vulnérabilités des outils numériques liés à l'e-learning et aux examens. Une vigilance renforcée est indispensable pour faire face à ces évolutions.

Renforcement par la formation : Élément clé de la résilience, l'erreur humaine demeure une vulnérabilité majeure. Les programmes de formation, les ateliers pratiques et les guides simplifiés contribuent à réduire les comportements à risque.

Disparités dans les investissements : Bien que les universités disposent souvent de budgets importants pour la cybersécurité, de nombreuses écoles, en particulier celles avec des ressources limitées, doivent faire des compromis entre l'acquisition d'équipements pédagogiques et la protection numérique. Encourager la mutualisation des ressources et le soutien financier ciblé pourrait aider à combler ces écarts.

Témoignages

des entrevues qualitatives

« Nous sommes une cible assez importante [pour les attaques de phishing et de ransomware], évidemment, l'éducation est une cible massive parce que nous avons l'argent du gouvernement et des académies derrière nous. »

École secondaire

« Nous voyons régulièrement des étudiants installer des logiciels à tout-va sans se rendre compte que leur compte a été compromis à cause d'une application Telegram piratée, ou qu'ils se sont inscrits à un service qui a été piraté. »

Collège d'enseignement supérieur

« Nous allons renforcer considérablement les mesures de sécurité figurant sur des listes de nombreuses petites choses à faire... nous allons imposer davantage de restrictions sur les comptes du personnel et des étudiants. »

Établissement d'enseignement supérieur

Résumé

Le secteur éducatif britannique affiche un niveau de préparation à la cybersécurité supérieur à la moyenne, porté par l'engagement des directions et la régularité des démarches de sensibilisation.

Toutefois, la gestion des chaînes d'approvisionnement, la rapidité d'application des correctifs et l'accès équitable à l'innovation technologique constituent des chantiers prioritaires, en particulier pour les écoles primaires et secondaires.

Pour rester résilient face à l'évolution des menaces, le secteur devra renforcer la collaboration, l'innovation et l'agilité dans ses réponses aux défis numériques.

Source

Département pour la Science, l'Innovation et la Technologie et Ministère de l'Intérieur. (2025). Enquête sur les atteintes à la cybersécurité 2025 : Résultats pour les établissements d'éducation. GOV.UK.

À Jour Avec Vos TI

PRIVAL®