

Résultats pour la campagne
de sensibilisation au Phishing
Nouvelle IA pour les
Étudiants du Secondaire 2

Établissement scolaire :
EPCA

Synthèse

La campagne de Phishing "ICT - Nouvelle IA / Neue KI" a été envoyée le 16 mars 2026 aux élèves du Secondaire 2 du canton du Valais via DiagnoPhish dans le cadre d'une démarche de sensibilisation à la sécurité informatique décidée par le Canton du Valais et coordonnée par l'Office de l'éducation numérique. Elle a été désactivée le 30 mars 2026.

Type	Phishing
Langues	Français et allemand
Utilisateurs	15845
Score de sécurité	83%

Un message émis par l'"Association des étudiants valaisans" (association qui n'existe pas) a été envoyé à tous les élèves dans la langue respective de leur établissement (français ou allemand). Le but du message était de donner un accès gratuit à "Intelligenza", un outil qui utilise l'intelligence artificielle, pour gagner en efficacité, écrire, résumer, résoudre des problèmes et réussir ses examens.

Les élèves étaient incités à cliquer sur un lien pour accéder à l'outil. S'ils cliquaient, ils arrivaient sur une page de login très similaire à O365. S'ils saisissaient des données, ils étaient redirigés sur une page de prévention avec quelques conseils.

Au total, 15'845 élèves ont participé à cette campagne. Ils ont obtenu un score de sécurité de 83% qui reflète leur capacité de résistance aux attaques de phishing. Un score de 100% correspond à une capacité de résistance totale.

Résultats

L'objectif du test était de vérifier si un tiers pouvait récupérer des données d'accès à l'infrastructure informatique (login/mot de passe). Ce sont des informations sensibles puisqu'elles permettent à un attaquant potentiel de pénétrer dans notre infrastructure en se faisant passer pour un utilisateur légitime.

Le message comportait plusieurs indices qui incitaient à la prudence :

- La provenance du message était floue.
- L'expéditeur était inconnu.
- L'offre était exagérément attractive. Elle se référait au MIT pour inspirer confiance.
- Le message cherchait à susciter un sentiment de besoin et d'urgence.
- L'interaction impliquait de se connecter à un site avec un login/mot de passe, mais on ne savait pas à quelle organisation appartenait la page.

Voici les résultats des élèves de votre établissement en comparaison à la totalité des établissements :

	Score total	Score de votre établissement
Nombre d'utilisateurs	15845	2058
% ayant cliqué sur le lien	14 %	11%
% ayant donné des données personnelles	9 %	8%
Score de sécurité	83 %	84%

La majorité des élèves qui a cliqué sur le lien a ensuite saisi des données alors qu'on leur demandait de se connecter (avec quels identifiants ?) à un site web inconnu.

Le score de sécurité est à considérer comme un indicateur de protection face à une attaque. Plus il se rapproche de 100%, plus la capacité à se protéger est bonne.

Une cinquantaine de destinataires ont répondu au message, soit par de simples commentaires ou emojis, soit par des messages plus élaborés dont voici un florilège :

Ne me faites pas perdre mon temps merci.
Bonjour, y a t'il réellement une IA pour réviser ou c'était juste pour nous faire perdre notre temps?
Bonjour, J'avais un question au sujet d'Intelligenza. Les donnés seront stockés où? Merci d'avance pour votre réponse. Avec mes meilleures salutations.
Et la vraie application elle est ou ?
Bonjour, Je vous remercie pour votre aide. Quel est le site pour y accéder ? Bien à vous
Bonjour, je ne savais pas à qui signaler ça, mais c'est un mail de phishing... Envoyé à beaucoup d étudiants avec un edu.vs.ch...
Le phishing c'est mal 🙄
Oui et moi jsuis une dinde c ça

<p>Ja BROO, müäsch nit uf die edu adress schicko, schüsch wäre scho safe scam gsi Trotzdem Funny Wieter eso!!</p>
<p>Hallo liebes "Intelligenzia"-Team, vielen Dank für diese überaus faszinierende Nachricht! Es ist wirklich rührend zu sehen, wie viel Mühe ihr euch gegeben habt, um uns Schweizer Studierende zu unterstützen. Ich bin besonders beeindruckt von eurem Zeitmanagement. Dass bei euch im März bereits das "Jahresende näher rückt", erklärt vermutlich, warum eure KI-Entwicklung dem Rest der Welt so weit voraus (oder hinterher?) ist. Vielleicht könnte das MIT-Tool mir auch dabei helfen, herauszufinden, in welchem Paralleluniversum wir uns gerade befinden? Es ist zudem erfrischend zu sehen, dass ihr euch nicht von lästigen Dingen wie "logischer Satzstruktur" oder "glaubwürdigen Absendern" (@myonlineaccount.vs) aufhalten lasst. Diese minimalistische Herangehensweise an die deutsche Grammatik ist sicher ein Vorbote für die Effizienz eurer Software. Ich würde mich ja liebend gerne anmelden, aber ich fürchte, mein Computer ist leider zu intelligent, um auf Links zu klicken, die so offensichtlich nach digitalem Sperrmüll riechen. Viel Erfolg weiterhin beim Üben – vielleicht schafft ihr es bis zum nächsten "Jahresende" im Juni ja, eine E-Mail zu schreiben, die nicht nach einem Schlaganfall von Google Translate aussieht. Hochachtungsvolle Grüsse, Ein Student, der tatsächlich lesen kann</p> <p>P.S.: Da sich euer Projekt doch unter der MIT Lizenz befindet, sendet mir doch gerne den Source-Code zum Projekt.</p>
<p>Wenn ich ohne KI auch nicht mehr denken könnte, würde ich auf den Link klicken. schiebt euch eure "KI" freundlich hinten rein :)</p>
<p>Bonjour monsieur (nom d'un enseignant d'informatique), Merci pour la piqûre de rappel mais je ne tomberai pas dans le panneau ;) ...ou devrais-je dire dans l'hameçon. Bonne journée !</p>
<p>Monsieur (nom d'un enseignant d'informatique), J'ai bien suivie votre cours sur le online fishing en 2ieme. Mes salutations les meilleurs Reynard Jeremy</p>
<p>Bonjour M. (nom d'un enseignant d'informatique), comment vous allez? Tout de bon 🙌</p>
<p>Hahahah tu ne m'auras pas! :]</p>
<p>Bonjour, Est il toujours possible d'y avoir accès en tant qu'étudiant ? Si la réponse m'est favorable, tenez moi au courant je suis très intéressé par votre modèle IA !</p>
<p>Bonjour, Bien vu pour le mail mais de nos jours beaucoup d'ados son préparer à ne pas donner leurs infos bancaires comme ça ! Mais merci pour l'expérience!! Meilleures salutations</p>

On observe plusieurs types de réponses : les personnes intéressées par le produit et les personnes qui ont remarqué que c'était du phishing. De plus, le nom d'un enseignant apparaît plusieurs fois. Ce dernier aurait donné un cours sur le phishing l'année passée... ce qui semble avoir porté ses fruits. A l'inverse, on observe, chez certains élèves, une tendance à répondre sur un ton provocateur au message. Ce réflexe, comme toute tentative de dialogue avec un attaquant (insultes, menaces ou ironie), devrait être fermement découragé. Répondre ne sert à rien. En répondant, on signale surtout que l'adresse est active, ce qui rend efficient l'envoi de davantage de messages du même type.

En dehors de ces réponses, difficile d'analyser les réactions des élèves. Il est possible qu'ils aient simplement supprimé le message, mais cela mériterait d'être vérifié si le sujet est repris en classe.

Difficile également de donner une analyse plus claire des compétences des élèves au vu du nombre élevé d'entre eux qui n'ont pas vu le message. La consultation des boîtes de courriels chez les élèves est en effet nettement plus faible que le corps enseignant et le personnel administratif et pédagogique.

Cette campagne est un bon outil pour aborder le thème du phishing avec les élèves, car elle reprend plusieurs ressorts classiques de ce type d'attaque :

- offre alléchante,
- ancrage local (association des étudiants valaisans),
- sentiment d'urgence,
- incohérences,
- le thème alléchant de l'intelligence artificielle.

Le message de prévention pourrait donc se concentrer sur des aspects très concrets :

- Comment repérer un message douteux ?
- Comment réagir face à un contenu suspect ?
- Que ne faut-il pas faire ?
- Quels sont les risques pour soi et pour la structure ?
- Quelle conduite adopter en cas d'incident ?

Quel que soit le score de votre établissement, il est recommandé de transmettre le contenu de ce rapport au corps enseignant qui pourra reprendre ce phénomène avec les élèves. De nombreux éléments utiles figurent d'ailleurs déjà dans ce rapport.

En cas de questions, n'hésitez pas à contacter le support de l'OEN.

Annexes

1. Le courriel envoyé :

Bonjour!

La fin d'année approche et tu vas te préparer aux examens finaux.

Mais tu ne sais pas comment gagner du temps pour faire tes résumés, notes de cours ou trouver des astuces pour mémoriser facilement.

La solution provient de l'Intelligence Artificielle.

Notre nouvel outil se nomme "**Intelligenza**" et a été développé par le MIT.

Avec cet outil, tu peux réécrire des textes manuscrits, résumer des documents, exercer tes connaissances et trouver des solutions à tous les problèmes, même en maths ou en chimie.

C'est ton outil pour réussir tes examens !

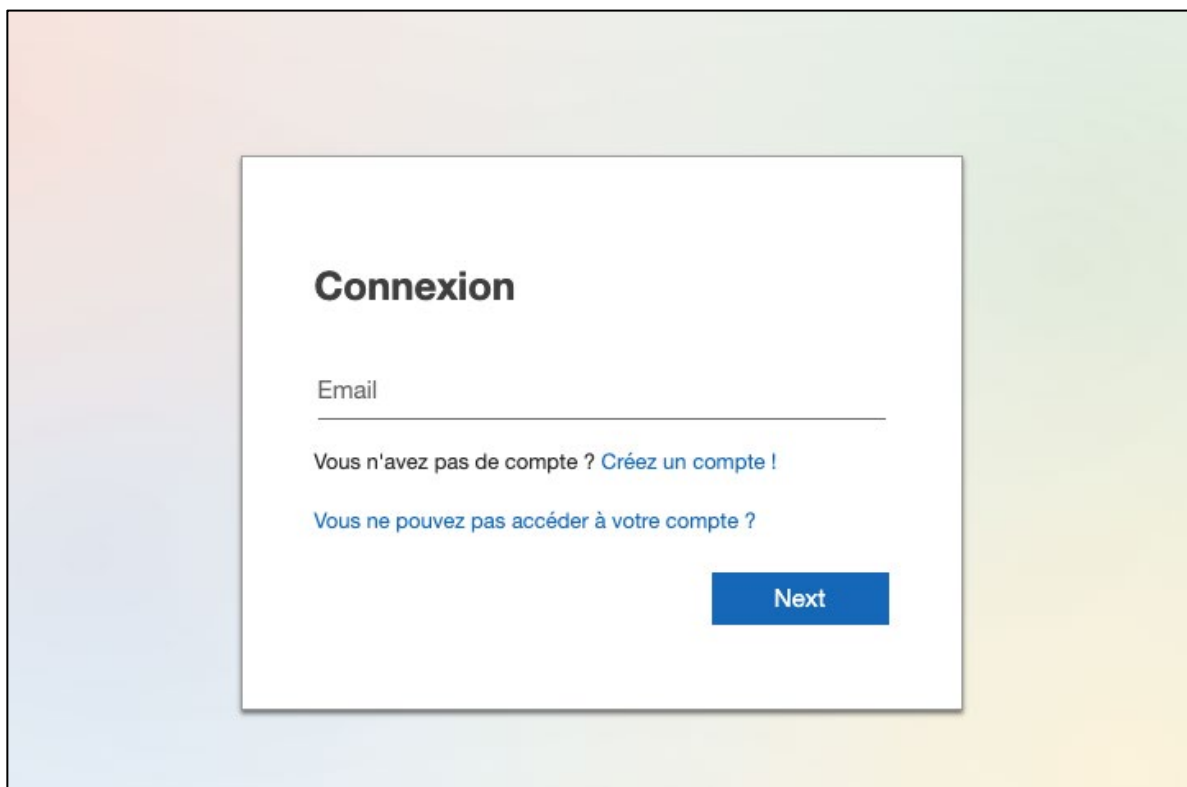
Et comme nous sommes en mars, **tu peux t'inscrire sur ce lien** pour y accéder gratuitement !

Tu as bien lu, c'est gratuit et c'est offert à tous les élèves de Suisse.

Alors inscris-toi sans attendre et profite de cet outil pratique et très facile à utiliser !

L'association des étudiants valaisans

2. La mire d'inscription



Connexion

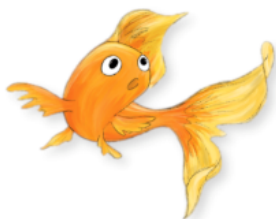
Email

Vous n'avez pas de compte ? [Créez un compte !](#)

[Vous ne pouvez pas accéder à votre compte ?](#)

Next

3. La page d'avertissement après avoir entré ses données de connexion :



Attention!

Vous avez été victime de phishing !

Dans le cadre de la campagne de sensibilisation définie par le Département de l'Economie et de la Formation (DEF) et mise en place par le centre de compétences ICT-VS, vous venez d'être soumis à un exercice de phishing. Le but est de vous apprendre à gérer les emails malveillants.

Ici, bien heureusement, pas de conséquences, car il s'agissait d'une simulation formatrice.

Néanmoins, nous vous recommandons de changer votre mot de passe dans les plus brefs délais.

C'est le bon réflexe à avoir après avoir rentré ses données de connexion sur un site malveillant.

Vous avez des questions ? Consultez notre page de support : <https://edu.vs.ch/assistance>

Vous pouvez fermer cette page à présent.

Le but n'était pas de vous piéger mais de vous donner l'occasion de prendre conscience des risques.

Merci de jouer le jeu et de ne pas avertir vos collègues! Ainsi l'exercice sera représentatif.

Lisez ces quelques conseils pour éviter de vous faire piéger dans le futur