Alerte Phishing

UNIVERSITÉ de Picardie Jules Verne

La DiSI vous informe

ATTENTION,

Vous êtes régulièrement amené à **recevoir de nombreux mails** vous incitant **à cliquer sur un lien,** afin de mettre à jour un annuaire, de réactiver votre webmail, votre mot de passe, etc. Il s'agit très certainement d'une **tentative d'hameçonnage (phishing).** Les pirates cherchent ainsi à **voler vos identifiants de connexion.**

CES MESSAGES NE PROVIENNENT PAS DE NOS SERVICES.

Nous vous invitons à **toujours VÉRIFIER CES 3 POINTS** si un mail contient un lien cliquable.

1. Avant de cliquer, vérifiez **l'adresse du site (url)** vers lequel ces mails renvoient **en survolant le lien avec la souris**. Les sites de l'UPJV se terminent toujours par **u-picardie.fr**
2. Avant de cliquer, vérifiez **le format du site web.** Les sites de l'UPJV sont toujours sur le format **site.u-picardie.fr**
3. Si vous avez cliqué sur le lien, vérifiez que l'adresse du site **commence par https, que le cadenas est présent** et **non barré** et que le navigateur n'indique **aucune erreur.**

Si vous avez l**e moindre doute** concernant **la fiabilité du site**, n'indiquez en aucun cas **vos identifiants personnels** et prenez contact avec la DiSI en **cliquant ici.**

*Si vous consultez vos mails **depuis votre smartphone** vous ne pourrez pas vérifier ces points.*
*Il est donc préférable **d'attendre d'être sur votre poste** pour effectuer ces vérifications.*

https://cas.u-picardie.fr
https://webmail.u-picardie.fr
https://pedag.u-picardie.fr
...

https://u-picardie.xyz.fr
https://abc.def.fr/u-picardie.fr
https://tinyurl.com/UPJV-cas
...

Si, malgré tout, vous avez **cliqué sur un lien douteux et entré vos identifiants**, vous devez **MODIFIER VOTRE MOT DE PASSE.**

1. **RENDEZ-VOUS SUR L'ENT DES PERSONNELS**
   cliquez (en haut à droite) sur le lien « *Activer mon email UPJV - Mot de passe oublié* »
2. **CLIQUEZ ENSUITE SUR L'ITEM DU MENU**
   « *J'ai oublié mon mot de passe* »

Vous pouvez aussi **contacter**, si nécessaire, **l'assistance téléphonique** de la DiSI au **03.22.82.59.29.**

Dans tous les cas, **la DiSI désactivera votre compte** s'il vient à être utilisé par les pirates.

5 CONSEILS POUR SE PROTÉGER DU PHISHING.

1. **SOYEZ TOUJOURS VIGILANTS**
   lorsque l'on vous demande vos données personnelles.
2. **N'OUVREZ JAMAIS UNE PIÈCE JOINTE**
   dont l'expéditeur est soit inconnu, soit d'une confiance relative.
3. **VÉRIFIEZ LES LIENS**
   en passant la souris au-dessus (sans cliquer) pour s'assurer qu'ils renvoient vers des sites de confiance.
4. **NE RÉPONDEZ JAMAIS SOUS LA PRESSION**
   de ce type de sollicitation et n'engagez pas vos données personnelles (identifiants, mots de passe, ...)
5. **CONTACTEZ L'EXPÉDITEUR PAR UN AUTRE BIAIS**
   au moindre doute, cela vous confirmera s'il sagit d'une tentative de fraude ou non.

Pour en savoir plus, cliquez **ici** pour consulter l'infographie dédiée aux **bonnes pratiques informatique.**