



La Lettre d'infos de KAZ

N°6 du 14 juillet 2023

*Le numérique pour tous,
sobre, libre, éthique et local*

Le mot de la Collégiale

La troisième saison de l'aventure KAZ commence avec une offre de services toujours plus complète mais toujours sobre, libre, éthique et locale.

Cette offre s'appuie sur une architecture matérielle et logicielle diversifiée, efficace pour des coûts bien maîtrisés.

1. Les abonnements et règlements

Les abonnements se poursuivent de façon régulière.

Pour autant, les renouvellements posent parfois problème. Les échéances ne sont pas toujours respectées. Ce qui tend un peu la trésorerie de l'association.

Ce n'est pas la plupart du temps de la mauvaise volonté. Les montants restent très peu élevés. Une raison principale à cela : un certain nombre de kaznautes ne relèvent pas leurs courriels envoyés à leur adresse @kaz.bzh. Ils continuent d'utiliser leurs adresses électroniques anciennes.

Les rappels d'abonnement sont envoyés aux adresses @kaz.bzh. D'où le problème.

Merci de vérifier votre situation et de découvrir si nécessaire, votre adresse électronique @kaz.bzh.

2. L'offre de services et ses évolutions

Le changement de mot de passe est désormais opérationnel.

Mot de passe perdu ou souhait de changer de mot de passe, rien de plus simple ?

Vous pouvez changer de mot de passe avec un mot de passe unique sur tous les services KAZ nécessitant un compte géré par Kaz : cloud général (cloud.kaz.bzh), les mail, l'agora et Mobilizon.

Aller sur <https://mdp.kaz.bzh> et choisissez votre nouveau mot de passe.

Les comptes gérés par les organisations elles-mêmes ne sont pas concernés par cette centralisation de gestion des mots de passe : clouds orgas (orga-cloud.kaz.bzh), les sites WordPress (orga-wp.kaz.bzh).

Une offre qui s'enrichit en permanence.

- **Un gestionnaire (coffre-fort) de mots de passe <https://koffre.kaz.bzh>.**
Bitwarden est l'un des **meilleurs** gestionnaires de mots de passe : gratuit et open source, il permet de stocker les identifiants de tous vos comptes web dans un **coffre-fort sécurisé** avec une facilité déconcertante ! De plus, grâce à son générateur de mots de passe, il permet d'**améliorer drastiquement la sécurité** de tous vos comptes sur Internet. Installé sur nos serveurs, nous l'avons baptisé « **Koffre** » .
Vous êtes certains que vos mots de passe sont à l'abri.
En ligne, votre coffre-fort est accessible sur tous ordinateurs, tablettes et smartphones.
Pour créer votre coffre-fort, aller à <https://koffre.kaz.bzh> .
- Pour les organisations, mouvements et collectifs, essayez « **Mobilizon** » pour l'organisation d'évènements et de gestion de groupes.
Lancé en octobre 2020 par [Framasoft](#) pour proposer une alternative libre aux plateformes des [GAFAM](#) (Facebook, Meetup.com, EventBrite), Mobilizon a acquis assez rapidement une grande visibilité dans les cercles de hackers, mais aussi rapidement au sein de la scène culturelle européenne et plus récemment dans les médias informatiques grand public.
Créez votre compte Mobilizon chez KAZ : <https://mobilizon.kaz.bzh>

3. L'architecture matérielle repose désormais sur deux sites de production.

Kaz a démarré il y a deux ans et demi en installant son système chez GRIFON, un hébergeur associatif situé dans la région rennais.

GRIFON : Groupe Rennais pour un Internet Fourni de manière Ouverte et Neutre.

Notre collaboration se poursuit avec GRIFON.

Toutefois par souci de diversification, nous avons choisi d'installer un deuxième serveur chez un autre hébergeur associatif FAImaison installé à Nantes.

Les performances techniques sont au rendez-vous.

4. Retenez la date 15 septembre 2023

C'est un vendredi à 18h00 à la Maison des associations à Vannes. Dans l'amphithéâtre.

Présentation de KAZ, sa finalité, ses objectifs, sa stratégie, sa gouvernance, les femmes et les hommes qui font KAZ, ...

5. Le programme de formation 2023-24

Les formations ont lieu le dernier vendredi de chaque mois de 18h00 à 20h00.

6. Sécurité des sites Wordpress :

La sécurité de votre site Wordpress est essentielle ! Des pirates peuvent vouloir l'utiliser pour escroquer vos visiteurs, ou le rediriger vers des sites illégaux... et quelques règles de base peuvent sécuriser votre site :

- * Supprimer dans Wordpress les comptes admin, webmaster... et pour les autres, s'assurer que les mots de passe sont bien considérés par Wordpress comme "forts".
- * Vous limiter à des extensions connues et utiles à vos besoins. Si le noyau de Wordpress est bien sécurisé, ce n'est pas toujours le cas des extensions.
- * Installer une extension pare-feu et surveillance de logiciels malveillants comme Wordfence.

Wordfence : destinée à protéger et à éliminer les menaces qui auraient pu s'installer sur un site Wordpress, cette extension inclut un pare-feu et un scanner de logiciels malveillants. il s'agit d'un Freemium, c'est à dire d'une extension qui dispose d'une version gratuite avec certaines limitations et d'une version Premium plutôt destinée aux professionnels. La version freemium est largement suffisante pour un site associatif avec un délai de mise à jour des signatures d'attaques de 30 jours.