

## Dans ce numéro

# Quoi de neuf?

### Faits saillants - Payworks

## Apprenez à les connaître

Apprenez à connaître votre représentant du service à la clientèle

## Sécurité sur Internet

La sécurité avant tout

# Quoi de neuf?

## Faits saillants - Payworks

### Produits du SGRH

Payworks a récemment annoncé les améliorations apportées à la composante Avantages sociaux du SGRH. Les modifications suivantes ont été apportées aux menus de configuration du SGRH et des avantages sociaux du SGRH :

- L'écran de configuration des avantages sociaux a été reconfiguré.
- La fonction « Calcul automatique/ Envoyer à la paie automatiquement » a été ajoutée à titre d'option de configuration dans l'écran de configuration des avantages sociaux.
- La configuration de la rubrique « Diagrammes de taux – Avant. Sociaux » a été simplifiée.
- L'écran d'adhésion en masse aux

avantages sociaux a été amélioré pour accommoder la fonction « Calcul automatique/Envoyer à la paie automatiquement ».

- L'écran « Couvertures des avantages sociaux » indique maintenant le taux de prime de la couverture et contient d'autres améliorations apportées aux fonctions.
- Les changements de salaire apportés dans les écrans « Payroll Pay Info/ Mass Pay Adjustments » et « Gestion du rendement SGRH » déclencheront la nouvelle fonction « Calcul automatique/Envoyer à la paie ».

Pour obtenir de plus amples renseignements sur les améliorations apportées à la composante avantages sociaux du SGRH, vous pouvez consulter les bulletins des produits de Payworks dans la section du

site Web de Payworks qui leur est réservée.

### Uniformisation des frais pour tous les paiements

Nous vous avisons que le 1er juin 2012, les frais des paiements suivants : Paiements - Retours/Révocations/Suivis, Révocations - Manuels, et des oppositions aux paiements ont été uniformisés à 7,50 \$ pour tous les types de paiement.

- Les frais des paiements - Retours/Révocations/Suivis ont augmenté, étant passés de 2,50 \$ à 7,50 \$.
- Les frais des rappels de paiements - Manuels ont diminué, étant passés de 20,00 \$ à 7,50 \$.
- Les frais des oppositions de paiements ont diminué, étant passés de 10,00 \$ à 7,50 \$.

Payworks  
mai/juin  
Bulletin

the  
works

Ce changement dans les frais ne constitue que le premier d'une série de changements qui auront lieu au cours des prochains mois et qui se transformeront en une base de données générale dont la date de lancement est prévue pour le 1er août 2012.

La base de données générale s'ajoutera aux outils actuels pour le traitement de la paie qui permettront aux clients qui traitent eux-mêmes leurs paies d'effectuer en ligne leurs propres oppositions aux paiements. Les clients auront également la capacité d'annuler un chèque non encaissé par un employé, de rediriger un TEF et de gérer les refus visant les TEF.

Si vous désirez de plus amples renseignements concernant les modifications apportées à la tarification, vous pouvez communiquer avec votre représentant du service à la clientèle au 1-866-788-3500.

# Apprenez à les connaître

## Get to know your Client Service Representative

Brittany Fiel est la coordonnatrice de la mise en application chez Payworks et travaille principalement dans le secteur des PME. Elle communique chaque semaine avec de 10 à 30 clients, parfois plus selon la saison. Elle est au service de Payworks depuis un peu plus de quatre ans.

Elle adore ses collègues et apporter son aide aux nouveaux clients. Les journées qu'elle préfère, ce sont celles où un client lui dit à quel point la transition à Payworks s'est déroulée en douceur et lui exprime sa satisfaction de nous avoir choisis!

Brittany travaille dans le domaine du service à la clientèle depuis qu'elle a 18 ans. Avant de rejoindre les rangs de Payworks, elle a travaillé comme maquilleuse et gérante. Dans le domaine du service à la clientèle, il faut aimer aider les gens et c'est une qualité que vous avez ou que vous n'avez pas. Heureusement pour nous, Brittany l'a!

Brittany est mariée depuis deux ans et elle et son mari possèdent deux chiens, Winston et Rosie. Winston est un chien berger à poils longs de trois ans et ils ont sauvé Rosie (probablement un chien croisé) en novembre.

Lorsqu'elle n'est pas au travail, Brittany aime courir avec ses chiens, faire de la photographie, offrir ses services à titre de maquilleuse, pratiquer la boxe orientale, danser le clogging, suivre des cours de toutes sortes (dont l'harmonica), voyager, cuisiner et acheter des chaussures... Brittany possède un peu plus de 100 paires de chaussures. Elle dispose également d'une pièce dans sa maison réservée au maquillage!

Brittany fera un voyage à New York en juillet et elle a très hâte! Au cours des dernières années, elle est allée au Mexique, à Cuba, en République dominicaine, au Panama et à Las Vegas. En avril dernier, elle a participé à un « congrès de clogging » au Manitoba.



Brittany Fiel  
Brittany Fiel, coordonnatrice de la mise en application

# Sécurité sur Internet

## La sécurité avant tout

Par Kevin Sokolowski, vice-président, Technologie de l'information, Payworks

Internet est un outil incroyable qui facilite les tâches quotidiennes à accomplir, mais qui permet aussi aux criminels informatiques d'exercer des activités frauduleuses. Voici des mesures que vous pouvez prendre pour protéger votre identité en ligne et empêcher que vous ne deveniez une victime de ces criminels.

Les mesures faciles suivantes vous aideront à vous protéger :

- Choisissez des fournisseurs de logiciels antivirus et de protection contre les logiciels espions et malveillants de confiance et assurez-vous que votre ordinateur est configuré de façon à recevoir automatiquement des mises à jour pour votre système d'exploitation.
- Assurez-vous de ne visiter que des sites Web officiels en utilisant des moteurs de recherche fiables comme Google ou Bing et de ne visiter que le site Web de la société, ou de visiter le URL du site de la société directement. Évitez de cliquer sur des liens qui peuvent être malveillants souvent contenus dans les courriels de hameçonnage qui vous dirigent vers un site ayant l'apparence d'un site officiel.
- Lorsque vous naviguez sur Internet, un message d'avertissement peut s'afficher vous avisant que votre ordinateur a été infecté par un virus et vous demandant de cliquer sur un lien pour installer un logiciel. Si vous recevez un message de ce genre, fermez tout simplement la fenêtre de votre navigateur et exécutez votre propre programme antivirus sur votre ordinateur. Il est fort probable que votre programme antivirus ne détectera pas d'infection.
- Lorsque vous entrez des renseignements personnels ou accédez à un site Web contenant vos renseignements personnels, assurez-vous que vous êtes connecté par un protocole SSL (c'est-à-dire dont l'adresse du site Web commence par https://). De nombreuses sociétés fournissent également des certificats de validation étendu pour leurs sites Web qu'il est possible de reconnaître par la

couleur verte dans la barre d'adresse. Dans le cas d'un certificat de validation étendu, la société qui a émis le certificat SSL a également vérifié l'identité de la société demandant le certificat.

- Idéalement, vous devriez utiliser des noms d'utilisateur et mots de passe différents pour chaque site Web que vous visitez. Si vous utilisez les mêmes noms d'utilisateur et mots de passe pour plusieurs sites Web, les attaquants qui réussiront à accéder à un de vos sites pourront également accéder à vos autres sites. Les réseaux sociaux offrent maintenant des liens entre les comptes des réseaux sociaux et les autres comptes pour faciliter la tâche aux utilisateurs; mais pour cette même raison, les comptes des réseaux sociaux sont très ciblés et il est préférable d'éviter d'utiliser les liens entre vos comptes et votre identité dans les réseaux sociaux.
- Utilisez des mots de passe FORTS. Les mots de passe forts ne sont pas toujours pratiques, mais ils offrent une excellente protection contre les attaques en force, lorsqu'un attaquant tente d'accéder à vos comptes en utilisant un scénario visant à trouver des mots de passe « courants ». Un mot de passe fort contient au moins 8 caractères, au moins une lettre en majuscule, au moins un caractère spécial (!@#%\$%^&\*()) et au moins un chiffre.

### Types d'attaque

#### Hameçonnage

Dans les attaques par hameçonnage, le site Web ressemble à s'y méprendre au site officiel d'une banque ou d'un fournisseur de la paie. Les attaquants tentent d'inciter les utilisateurs à visiter ces faux sites par l'envoi de courriels ou de messages textes ou par des appels téléphoniques. L'utilisateur qui visite un site fictif et y accède en entrant ses justificatifs d'identité se fait voler ces justificatifs par l'attaquant qui les utilise pour accéder au vrai compte de l'utilisateur.

#### L'attaque de l'homme du milieu (HDM)

Ce type d'attaque survient habituellement par l'infection de l'ordinateur d'un utilisateur par un logiciel malveillant. Ce logiciel redirige les demandes sur le Web vers le site de l'homme du milieu, qui fait ensuite parvenir les demandes au site légitime. Dans ce type d'attaque, les demandes sont interceptées et peut-être modifiées avant de parvenir au site légitime. En utilisant un logiciel de protection contre les logiciels malveillants d'un fournisseur de confiance, il est possible de se protéger contre ce type d'attaque.

#### Man in the Browser (MitB)

Ce type d'attaque est une variante de l'attaque de l'homme du milieu, mais au lieu de se baser sur un logiciel malveillant installé dans l'ordinateur de l'utilisateur qui est plus facile à détecter, un module externe de navigation malveillant est vraiment installé dans l'ordinateur ciblé. Ce module externe n'est activé que lorsque l'utilisateur visite les sites Web ciblés et est très difficile à détecter en raison de sa capacité à se fermer et à s'ouvrir au besoin. Comme ce module d'extension est hébergé dans le navigateur, il laisse une empreinte beaucoup moins suspecte et plus difficile à détecter. La façon la plus simple de se protéger contre ces types d'attaque est de désactiver les modules externes, ce qui empêche les logiciels de s'activer. Une autre façon consiste à installer un logiciel de sécurité pour la navigation sur Internet comme Trusteer's Rapport (<http://www.trusteer.com/product/trusteer-rapport>).

À titre de fournisseur de services, nous faisons tout notre possible pour protéger vos données lorsque nous les manipulons, et à titre d'utilisateur, vous pouvez faire la même chose en protégeant votre ordinateur et en vous renseignant. Si vous apprenez à connaître les types de menaces qui existent, vous pourrez plus facilement protéger vos renseignements confidentiels. Si vous doutez du courriel ou du site Web qui est censé provenir de votre fournisseur de services (Payworks, votre banque, votre société émettrice de carte de crédit, etc.), prenez le temps de communiquer avec lui et de vous informer. Nous sommes là pour vous aider. ○

## 30<sup>e</sup> congrès annuel et salon professionnel de l'APC

Du 2 au 5 juillet, des spécialistes en traitement de la paie de tout le Canada se réuniront lors du plus important salon professionnel dans le traitement de la paie au Canada.

Le 30<sup>e</sup> congrès annuel et salon professionnel de l'Association canadienne de la paie (ACP) « Tirez profit du professionnalisme de la paie » aura lieu en juillet au Centre des congrès d'Ottawa, en Ontario.

Payworks étant l'un des principaux promoteurs de cet événement prestigieux, nous vous invitons à participer à ce congrès et ce salon professionnel, à venir nous saluer au kiosque de Payworks (numéros 207 et 306) et à participer au concours pour gagner l'un de nos fabuleux prix!

Payworks parrainera également le Canadiana Snack Food Break pendant le salon professionnel, le mardi 3 juillet, de 14 h à 16 h. Le Snack Food Break offrira aux délégués des échantillons des différentes collations typiques du Canada. Nous avons très hâte de participer à cette activité!

Pour obtenir de plus amples renseignements ou pour vous inscrire au congrès de l'ACP, vous pouvez visiter le site Web de l'ACP à [www.payroll.ca](http://www.payroll.ca).

