Payworks
May/June
Newsletter

the works

Inside this issue

What's New?

Payworks Highlights

HRMS Product Update

Payworks has released enhancements to the HRMS Benefits component. The HRMS Setup and HRMS Benefits menus were modified, including the following:

- The Benefit Coverage setup screen was reconfigured;
- 'Auto Calculate' and 'Auto Send to Payroll' functionality was added, as a setup option, to the Coverage Setup screen;
- The Benefit Rate Chart setup was simplified;
- The Mass Benefit Enrollment screen was enhanced to accommodate the 'auto-calculate' and 'auto send to payroll' functionality;
- The Employee Benefit Plan Coverage screen now displays the coverage rate premium and contains other functional enhancements; and
- Wage changes made through the Payroll Pay Info / Mass Pay Adjustments and HRMS Performance Reviews screens will trigger the new Auto Calculate/Send to Payroll functions.

For more information on the enhancements in Payworks HRMS Benefits, please view the complete product bulletin in the Company Bulletins section of the Payworks Portal Page.

Stop Payment Price Changes

Please be advised that as of June 1, 2012, the charges for the following payments: Payment - Returns/Recalls/Traces, Payment Recall - Manual, and Stop Payments were standardized to a flat fee of $7.50 for each payment type.

- The charge for Payment - Returns/Recalls/Traces increased from $2.50 to $7.50.
- The charge for Payment Recall - Manual decreased from $20.00 to $7.50.
- The charge for Stop Payment decreased from $10.00 to $7.50.

This price change is just the first step in a series of changes taking place over the next few months, culminating in a Trust Database that is expected to go live on August 1, 2012.

The Trust Database is an enhancement on the current payroll tools that will allow those clients who currently run their own payrolls to manage their own stop payments via the web, including: the ability to cancel an employee's uncashed cheque, redirect an ETF, and manage ETF rejections.

If you have any questions or concerns regarding the pricing changes, please contact your Customer Service Representative at 1-866-788-3500.

Get to Know Them

Get to know your Client Service Representative

Brittany Fiel is the Implementation Coordinator at Payworks, and she works mostly within the Small Business sector. She contacts anywhere from 10 to 30+ new clients per week, depending on the season. Brittany has worked for Payworks for just over 4 years.

Brittany adores her coworkers, and she loves getting to help out new clients all of the time. Her ideal day would end with a client telling her how easy she has made their transition to Payworks, and how happy they are to come on board with us!

Brittany has been in the customer service industry since she was 18. Before coming to Payworks, she worked as a makeup artist and a manager. She feels like Customer Service, and a love of helping people, is something you either have, or you don't. Luckily for us, Brittany does!

Brittany has been married for two years, and she and her husband have two dogs, Winston and Rosie. Winston is a 3-year-old long haired Sheppard, and they rescued Rosie (they believe she is a lab mix) in November.

When she isn't at work, Brittany enjoys taking her dogs for runs, photography, freelance makeup, kickboxing, clogging, taking random classes (harmonica lessons), traveling, cooking, and buying shoes. She has just over 100 pairs of shoes. Brittany also has a room in her home dedicated to makeup!

Brittany is going on a trip to New York in July and she is **very** excited! In past years, Brittany has traveled to Mexico, Cuba, the Dominican Republic, Panama, and Las Vegas. This past April, Brittany attended a "clogging convention" in Manitoba.

Brittany Fiel
Implementation Coordinator

Payworks
May/June
Newsletter

the works

Internet Security

Safety First

By Kevin Sokolowski, Vice President, Information Technology at Payworks

The Internet is an incredible tool that makes it easier to accomplish many kinds of tasks on a daily basis, but in doing so, it also opens a new world for criminals to attempt to steal from you. We have identified some steps you can take to protect your online identity and to prevent yourself from becoming a victim to online criminals.

Here are some simple things that you can do to protect yourself online:

- Ensure you are running anti-virus and anti-spyware/malware software from a reputable vendor, and ensure your computer is set to automatically receive updates for your Operating System.
- Verify that you are visiting an official website by using a reputable search engine like Google or Bing and searching for the company's website, or visit the URL to the company's website directly. Avoid clicking on potentially malicious links often contained within Phishing emails that direct you to a website impersonating an official website.
- As you are browsing the Internet, a warning message may pop up with a notice that your computer is infected with a virus and requiring you to click a link to install software. If this occurs, simply close your browser windows, and run your own anti-virus scan on your computer. It is most likely that your anti-virus software will not detect an infection.
- When entering personal information, or accessing a website containing your personal information, ensure you are connected via SSL (the website address will begin with https://). Many companies are also providing Extended Validation certificates for their websites, which you can recognize by the "green" colour in the address bar. Extended Validation certificates mean that the company that issued the SSL certificate also verified the identity of the company requesting the certificate. Example:

- Ideally you should use a different login and password for each website you use. When usernames and passwords are shared across different websites, attackers who steal your log–in to one site will also have access to your other websites. Social networks now allow you to "link" your Social Network accounts with other accounts to make it more convenient for users; as a result, Social Network accounts are highly targeted for theft, and it is best to avoid "linking" accounts to your Social Networking identity.
- Use STRONG passwords. Strong passwords may be inconvenient at times, but they provide excellent protection against brute force attacks, whereby an attacker attempts to access your accounts by running a script that attempts to find "common" passwords. A strong password is at least 8 characters in length, contains at least one capital letter, at least one special character (!@#$%^&*()), and at least one number.

Types of Attacks

Phishing

A phishing attack begins by the attackers setting up a website to look like the official website of a Bank or Payroll Provider. The attackers then attempt to trick users into visiting these fraudulent websites through emails, text messages, or over the telephone. If the user visits this phony website and attempts to log in with their credentials, the login information is stolen and used by the attacker to access the user's real account.

Man in the Middle (MitM)

This type of attack is usually instigated through the infection of a user's computer by malware. This malware will reroute web requests to a "Man in the middle" website, which will then forward the requests on to the legitimate website. In this type of attack, the requests are monitored and possibly altered before being submitted to the legitimate website. Using a reputable third party anti-malware software solution is sufficient to protect against this type of attack.

Man in the Browser (MitB)

This is a variant of the MitM attack, but rather than relying on more easily-detected malware installed on the user's computer, this type of attack actually installs a malicious browser plug-in on the target's computer. This plug-in is only activated when the user visits targeted websites, and is extremely hard to detect due to its ability to turn itself on and off as needed. Because the plug-in lives in the browser, it leaves a much less suspicious footprint for anti-malware software to detect. The easiest way to prevent these types of attacks is to browse with "Plug-ins" disabled, preventing the malicious programs from being activated. Another way to prevent these attacks is to install browser security software such as Trusteer's Rapport (http://www.trusteer.com/product/trusteer-rapport).

As a service provider, we do our best to protect your data while it is our hands, and as a user you can do the same by protecting your computer, and by educating yourself. If you arm yourself with the knowledge of what types of threats are out there, you can better protect your private information. If you are ever uncomfortable or unsure about something in an email or website that seems to be from your service provider (Payworks, your bank, your Credit Card company, etc.), take the time to contact your service provider and ask them about it. We are all here to help.

The CPA 30th Annual Conference & Tradeshow

On July 2-5, payroll specialists from across the country will gather at the largest payroll trade show in Canada.

The Canadian Payroll Association's (CPA) 30th Annual Conference and Tradeshow: Capitalizing on Payroll Professionalism takes place this July at the Ottawa Convention Centre in Ottawa, ON.

Payworks is a gold sponsor of this prestigious event, and we invite you to attend the conference and tradeshow and stop by the Payworks booth (numbers 207 & 306) and enter to win our great prizes!

Payworks is also sponsoring the Canadiana Snack Food Break during the trade show, from 2 PM until 4 PM on Tuesday, July 3. The Snack Food Break provides delegates with a taste of Canadian snack offerings. We look forward to participating in the celebration!

For more information, or to register for the CPA conference, please visit the CPA website at www.payroll.ca.