5 INFORMATION SECURITY TIPS

FOR PAYROLL PROFESSIONALS

By Kevin Sokolowski

Confidential payroll and employee data should be some of the most highly-guarded information that organizations own. As technologies improve and become increasingly pervasive in every aspect of business, organizations must continually enhance their information security practices to keep data secure. Management teams, particularly those dealing with confidential employee information, need to set the standard for acceptable information security practices in their organizations and lead by example.

Here's a guideline for simple, but effective, ways that you can incorporate information security practices into your workplace.

1) SECURITY AWARENESS TRAINING

The topic of Information Security inevitably comes up when I talk to managers in other organizations, and there is a common misconception about how best to defend your organization from a data breach. Cyber and information security often invokes mental images of groups of hackers here and abroad working to break down the front door of your technology infrastructure. While this type of attack does happen, it is not as common as you may think. Recent high profile security breaches have led to many organizations establishing good perimeter defenses and budgeting for continual improvements. Having active defenses is great, but your organization cannot solely rely on them for full protection. Even the strongest, thickest walls are useless if someone invites the enemy through the front door - just ask the people from the city of Troy.

This is why I believe providing all employees with security awareness training is one of the most useful practices that organizations can employ to improve their overall security. There are many resources available to assist you in creating a comprehensive security policy and then educate your staff. Security awareness training is most effective if employees understand its importance and how it applies to your business. Educated and alert employees help mitigate the risk of a technology and/or physical security breach.

2) PASSWORD MANAGEMENT

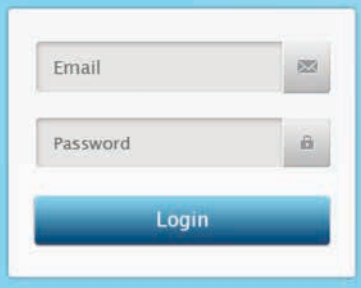
Passwords are one of the most familiar and routine information security methods. Even with advances in authentication methods, you likely still need passwords for many systems, from your email to your Canadian Payroll Association online sign-in. Because passwords are so common, people are often quite complacent about them. Failure to follow effective password standards can put company information systems and resources – or your own personal information – at risk.

Keep your passwords confidential at all times, and avoid using the "remember password" feature. Change your password often, and make sure you are changing to an entirely new password. Don't reuse password for multiple applications, and don't store passwords in a file on your computer or mobile device without encryption.

THE DOS AND DON'TS FOR CREATING STRONG PASSWORDS

[DO]

- + Use 15+ characters. The more characters used, the harder to crack or guess.
- + Use random words and numbers.
- + Use upper and lower case letters.
- + Use special characters and symbols.



[DON'T]

- − Use the same character for the entire password or fewer than five unique characters.
- − Use a variation of your login.
- − Use words, numbers, or public information associated with you (e.g. family names, pets, birthdays, phone numbers, or addresses).
- − Use a single word as your password (e.g. password). Non-English words are equally insecure.
- − Use common letter or number patterns (e.g. 123456 or qwerty).
- − Use substitution on common words (e.g. 3=E, 4=A, 1=I, 0=O, p455w0rd)

[IN THE CURRENT CLIMATE OF INFORMATION SECURITY, ESPECIALLY IN THE PAYROLL PROFESSION, WE ARE ALL RESPONSIBLE FOR KEEPING OUR DATA SECURE.]

3) ANTI-MALWARE

There are many varieties of malware and viruses, each with a different purpose. The best way to defend against these programs is to ensure that you have installed anti-malware software on your computer. Because it is widely accepted that no single technology can provide adequate protection from today's sophisticated network attacks, information security experts recommend that you use a layered approach of tools to protect your information, including firewalls, email security, anti-virus software, and anti-malware software. Security firms report that between 250,000 to one million new malware variants are released every day; it is critical that these tools be kept up-to-date.

4) REDUCE PAPERWORK

It can be difficult and sometimes inefficient to eliminate all paper from business processes; however, as much as possible, you should stop printing unless it is vital that you do. Most vendors offer self service functions that allow employees to view their pay statements and year-end forms securely online. Not only is a paperless solution more secure, it is also environmentally-friendly and can be more cost-effective than printing. If you do need to print, ensure that you shred all paperwork immediately after use. Papers left lying around or sitting in garbage cans are easy targets for data thieves.

5) EVALUATE YOUR WORKSPACE

This last step is a personal one. Questions you should ask yourself include: do you keep your work out in the open or leave papers on your desk? Does your computer lock after sitting idle? Who has access to your files and desk when you aren't around? Are there materials that should be locked up? Create your own strategy for maintaining information security and stick to it.

In the current climate of Information Security, especially in the payroll profession, we are all responsible for keeping our data secure. As attacks become more sophisticated, it is no longer solely an arms race of technology, but of processes and people as well. Data thieves have realized that attempting to exploit technology alone is far less effective than acquiring information from your people, which is why having an alert workforce is key to successfully keeping your data safe. With a comprehensive security policy and training, you and your employees will be equipped to keep all confidential payroll data and personal information secure. ■

Kevin Sokolowski is the Vice President, Information Technology at Payworks. Payworks is a national leader in the field of total workforce management solutions, providing online solutions for payroll, human resources, and employee time management to more than 13,000 businesses across Canada. For more information, visit payworks.ca.