Online Banking Safety

Tana Christianson, Director of Insurance

Sometimes, we come across an article published by other Canadian law societies and their insurers that is so good it really should be shared. The following article is by Dan Pinnington, Vice President of Claims Prevention at practicePRO, the professional liability insurer for Ontario lawyers. This article first appeared in the December 2013 issue of LawPro magazine. Kathy Levacque, Director of Audit for the Law Society of Manitoba, reminds you that the Law Society of Manitoba requires online access to law firm trust accounts be 'read-only'.

Increasing Your Online Banking Safety

by Dan Pinnington June 27, 2014

Many law firms manage their trust and regular bank accounts on the Internet. Some firms have the ability to initiate various banking transactions online, including account transfers and wiring funds. While the convenience and efficiency of online banking are huge benefits, the downside is that online banking exposes you to security risks. The steps outlined below will help law firms understand, address and reduce online banking risks – for both your firm and personal accounts.

- Know and understand the terms of your banking agreements: As a starting point, carefully read your bank account and electronic banking services agreements. Make sure you understand the obligations these agreements place on you with respect to using the account. In particular, make sure you are familiar with the notice requirements for unauthorized transactions, and who is responsible for unauthorized transactions. In most circumstances it will be you, unless in specified and usually narrow circumstances you give prompt notice to the bank.

- Remove account features you won't use: If hackers ever managed to get into your account, the ability to access multiple accounts or to initiate transfers or send wires could allow them to easily remove funds from your account. If you don't intend to use your online banking facility for these types of transactions, have this functionality removed from your account.

- Only do online banking from a secure firm computer: The computer used for online firm banking should be a firm computer that has all software updates installed, is running updated anti-malware software, and is behind a firewall. To reduce the potential for other cyber risks, consider restricting the activities that occur on the computer used for online banking.

- Have real-time protection running and run regular malware scans on your banking computer: This should hopefully help detect an infection as it is happening, or detect one that occurred without triggering the real-time protection warnings.

- Never use public computers to do banking for the firm: If doing so, passwords or account data may be accidentally stored on the computer or captured by malware making it accessible to others.

- Never conduct financial transactions over an unsecured public Wi-Fi network: Communications on an unsecured Wi-Fi connection can easily be intercepted.

- Use a secure and unique password that is changed regularly: Your online bank account should not have the same password as any other account. It should be a strong password. Online banking passwords should never be stored on a mobile device or anywhere else that could make them easily accessible by another person.

- Check your online bank account every day: By monitoring your daily account activity, you'll be able to promptly identify any unauthorized transactions or other indications that your account has been hacked. Check the last login time and make sure it is consistent with the last time someone from your office accessed the account. Immediately report suspicious or unexplained activity to your bank.

continued...

Online Banking Safety

...continued

- Configure email or text message activity alerts: Most banking websites allow users to sign up for notifications. You will then receive an email or a text message whenever a specified amount of money is withdrawn or deposited to your account, or if there is unusual activity such as international transactions. Some banks will also phone a firm for confirmation that a transaction that was initiated online is to go through.

Dan Pinnington is the Vice President of Claims Prevention at practicePRO. This article first appeared in the December 2013 issue of LawPro magazine. Reprinted with permission. For more cyber safety tips, visit www.lawpro.ca.