



For immediate release – January 27, 2015

Protecting your data in a wired world

Social media sites can be both a boon and a bane to our online networking. They are useful on a business and personal basis for many reasons but managing privacy and security requires serious attention, says Kevin Vadnais, information security manager at the University of Lethbridge.

Data Privacy Day on Wednesday, Jan. 28 is an international initiative that presents the opportunity to remind people to take a moment to update passwords and review privacy settings on sites like Facebook, Twitter and LinkedIn, says Vadnais.

“When we talk about data and data privacy, the first thing people think about is social media sites, and the privacy default settings for them are generally pretty wide open,” he says. “The level of security you need depends on what group you’re trying to reach. If you’re using social media as a marketing tool or as a communication medium, you do want it to be as public as possible. For your personal information, you want it restricted to probably friends only to prevent snooping eyes.”

Since the various sites regularly change privacy settings and options, the aim is to periodically check your settings to determine who can see and reply to your posts, who can view your photos, and what kind of personal data is available. Typically, the terms of service for such social media sites indicate that pictures, videos and text posted to the site can be deemed intellectual property and used at the company’s discretion.

“Essentially you give up the right to anything you post on social media sites. That’s the cost for using the service,” he says. “We need to be careful about what we put on the Internet and we need to rid ourselves of the illusion that if we put something up there by mistake it can be taken down. It can’t – the Internet is forever. A rule of thumb is if you don’t want it to appear on CNN then don’t post it.”

Vadnais adds that people should be aware social media sites are not charitable organizations. They are businesses that need to make a profit.

“If we are not paying for the service, we are not the customers. We are the product. Our information is being bought and sold by these organizations and we explicitly consent to

it when we join. Even the smallest amount of information can be used for nefarious purposes. Be very mindful of the data you're sharing," says Vadnais.

Not only online information needs to be protected. Safe disposal of old computers and devices is also important. Data that has been deleted can still be recovered. And resetting a computer back to its factory default settings doesn't necessarily mean the files can't be recovered. Hard drives should be removed and drilled through to break the platter inside before disposing of old equipment.

"In addition, organizations should not be collecting your data without disclosing how they plan to use it," says Vadnais. "They must disclose its use at the time of data collection and get explicit consent to use it in that manner."

The collection, use and disclosure of personal information and access to personal records are governed under the Freedom of Information and Protection of Privacy (FOIP) Act in Alberta.

In a nutshell, Vadnais suggests people check their social media settings, change passwords on a regular basis and be cautious about using pirated or illegal software. They should also research the companies and products they want to use to ensure they're reputable and have privacy practices that align with Canadian standards.

"If it's free it's probably free for a reason," he says.

-- 30 --

Contact:

Kevin Vadnais, manager of Information Security
403-322-4056
kevin.vadnais@uleth.ca

Caroline Zentner, public affairs advisor
403-394-3975
403-795-5403 (cell)
caroline.zentner@uleth.ca