Authorized Access

Information Privacy and Security Best Practices webinar

Facebook and Cambridge Analytica

Approximately 87 million Facebook users who did not have strict privacy settings configured had their account data surreptitiously harvested as a result of a personality quiz taken by 32 thousand other Facebook users. The data was analyzed for political leanings and susceptibility to advertisement-based influence. This software was purportedly used in 2016 to influence the Brexit referendum and the American federal election. **Takeaway:** Base social media engagement decisions on the understanding that indefinite procurement of your personal information are the providers' primary objectives.

Terms of Service

All social media and messaging services provide a Terms of Service statement that must be agreed to, typically in the form of a checkbox, to complete account creation. It outlines their right to utilize your profile, postings and messaging content in any form they see fit, without further consent. It is the actual rather than monetary price to be paid. Most people do not read it. **Takeaway:** Read the agreement before checking the box.

Phishing

Emails containing hyperlinks and instructions to click on them should be treated with caution. To verify their validity, first note the senders' address and domain, i.e. 'noreply@apple.com'. Then, hover your mouse pointer over the hyperlink taking great care to not click it; its actual URL will appear near it. If the URL's domain (i.e. 'apple.com') does not match the sender's address the email is likely a phishing trap. **Takeaway:** Verify the source of all communiques containing hyperlinks before clicking on them.

Public WiFi

Online accounts of any type should never be logged into using a public WiFi service without the protection of a VPN (virtual private network). Without its protection, unencrypted WiFi traffic that may contain your usernames and passwords could be captured by another computer within broadcast range of your device that is utilizing a program called a 'sniffer'.

Takeaway: Familiarize with and begin using a VPN for private and secure communications, and with the encryption feature when exchanging financial, legal, medical and all other confidential documents.

Nothing To Hide

A common misconception for social media users is that all thoughts and images are appropriate for posting to social media if they contain no apparent wrongdoing. However, each item contains clues that, in aggregate, can identify vulnerabilities and generate risks. **Takeaway:** 'nothing to hide' means 'nothing to protect'.

Rationalizations

Excuses or 'exemptions' that social media users commonly give themselves for sending risky content include "it was private", "no one can prove it was me" and "it's not against the law". In most situations these ideas are false. All of our messages and images are placed on the server hard drives of corporations. **Takeaway:** Messages can be traced to source.

Authorized Access

Information Privacy and Security Best Practices webinar

Safeguards

- Passwords should be easy to remember, difficult to guess, not about you and at least 12 characters.
- Review app permissions after installation and disable all unreasonable access to your personal information.
- Configure all privacy settings to 'friends-only' or equivalent.
- Determine if your needs are best met by a social media page (an advertisement) or simple texting.
- Be vigilant about verifying and accepting contacts.
- Be discrete about messaging content and avoid creating unnecessary data points.
- Limit the amount of time spent in social media; boredom creates risk.

Hierarchy of Messaging Privacy

Messaging external to and from the organization won't be subject to the same protections as those entirely within the same email server. This could include an exchange between organizational and personal accounts. Unencrypted messages can be intercepted at multiple points within the world-wide-web.

Takeaway: Determine the most appropriate method (see accompanying table) based on the message confidentiality and the potential for residual copies of the message left in the possession of service providers.

COMMON TERM	EXAMPLE	PROTOCOL
Browser	TOR	IP
VPN	Windscribe	IP
Message Encrypter	Signal	IP
Email Encrypter	ProtonMail	IP
Document Encrypter	Zarchiver	IP
Snailmail	Letter	Postage
Landline	Bell	Circuit
Cell phone	Rogers	4G
Texting	FB Messenger	IP
VOIP	Rogers	IP
Texting	Bell	SMS
Email	Gmail	IP
Social Media - Private	Facebook	IP
Social Media - Public	Facebook	IP

Steve Chapelle has been providing information privacy and security education to Canadian organizations since 2006. Prior to that he spent over 20 years in information technology management, analysis and customer service, primarily in the financial services sector. Information management experience has included security, availability and disaster recovery planning. He is also an instructor and developer at the Udemy and Skillshare online course platforms, and has written a book about the Spanish Flu pandemic, 'No Decision: The 1919 Stanley Cup Final', available at Amazon.

416.467.6856 | steve@stevechapelle.ca | www.stevechapelle.ca