Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

s.16(2)(c)

s.21(1)(a)

From:
Sent: July-09-19 4:21 PM
To: Foreman, Ryan
Cc:
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Thanks, Ryan,

The overall thrust of this guidance is fine (making sure the application is hosted and developed in countries with similar privacy and security outlook as Canada is especially helpful).

proof-v03-1920-...

From: Foreman, Ryan
Sent: July-09-19 1:08 PM
To:
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Sure – here's the draft publication that will be posted on the Cyber Centre web site. There are a few more changes in progress to the document.

Ryan

<< File: proof-v03-1920-0624-cyber-centre-social-media-chat-apps-e.pdf >>

From:
Sent: July-09-19 11:32 AM
To Foreman, Ryan
Subject: RE: WeChat Inquiry

s.15(1) - DEF

s.21(1)(a)

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hey Ryan;

May I take a look at your communication related to WeChat?

From:
Sent: July-09-19 11:29 AM
To:
Foreman, Ryan

Subject: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hi

In the discussion this morning, you had asked if CSE currently has any official Advice and Guidance (A&G) regarding WeChat.

I understand that Ryan's group has some generic A&G,

Is SITE asking for something more official?

At present,

Foreign use of this product should be limited to unclassified data only. CSE does not specify how WeChat should be used in individual counties as this more in the mandate of GAC.

We can dig into this one more if required.

Thanks

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

s.21(1)(a)

Sure – here's the draft publication that will be posted on the Cyber Centre web site. There are a few more changes in progress to the document.

Ryan

<< File: proof-v03-1920-0624-cyber-centre-social-media-chat-apps-e.pdf >>

From:
Sent: July-09-19 11:32 AM
To: Foreman, Ryan
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hey Ryan;

May I take a look at your communication related to WeChat?

From:
Sent: July-09-19 11:29 AM
To:
Foreman, Ryan
Subject: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hi

In the discussion this morning, you had asked if CSE currently has any official Advice and Guidance (A&G) regarding WeChat.

I understand that Ryan's group has some generic A&G,

Is SITE asking for something more official?

At present,

Foreign use of this product should be limited to unclassified data only. CSE does not specify how WeChat should be used in individual counties as this more in the mandate of GAC.

We can dig into this one more if required.

Thanks

Divulgé en vertu de la loi LAI - renseignements non classifiés

[redacted]

Pages 5 to / à 6

are duplicates

sont des duplicatas

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

CANADIAN CENTRE FOR
CYBER SECURITY

SECURITY TIPS FOR INSTANT MESSAGING, TEXTING AND SOCIAL MEDIA

SOCIAL MEDIA and instant messaging services such as Facebook, Twitter, WhatsApp, Skype, and WeChat give you the power to connect with others effortlessly and share information instantly. But using these services can provide threat actors easy access to your information and devices. You can even be placing your online identity and that of your colleagues at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use, you need to consider both the functionality of the service and how secure and private your information and activity will be.

SIX FACTORS TO CONSIDER IN ASSESSING THE RISKS OF USING A PARTICULAR SERVICE OR APP:

Ensure you're using a service or app from a trustworthy platform. An app can have a high profile online and be useful, but somewhere there's a company operating that service, accessing your device and holding your information. You need to decide if you trust the platform to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

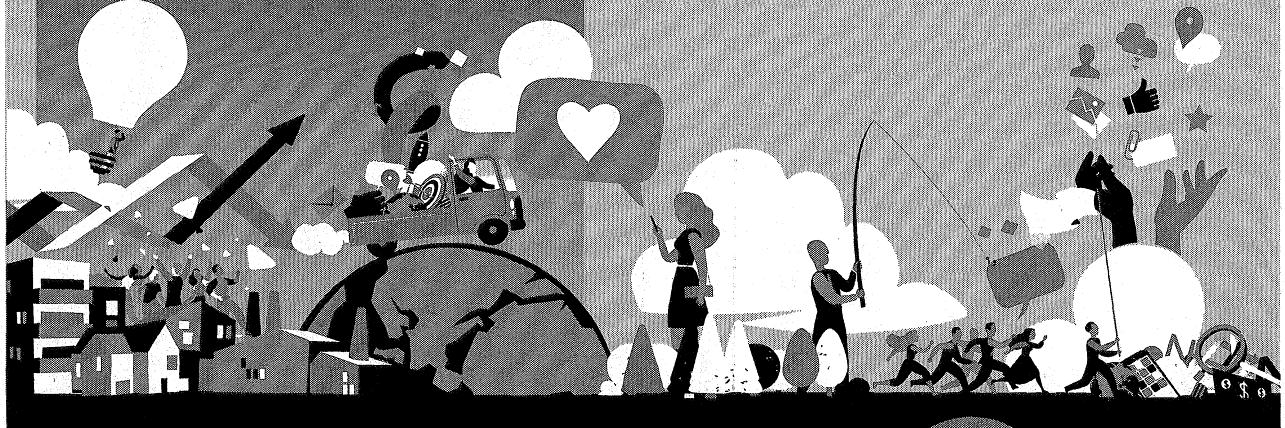
Pay close attention to the app or platform's security functions. Don't use a platform that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide fast support if your account is compromised.

Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously.

Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the platform of the service you are using.

If you feel you require an app or service but aren't sure of how secure it is, consider having a phone or computer dedicated to that app. Don't use the device for anything else, and never use it for sending sensitive information, even by direct message.

Think about which nation's laws will apply to your information and your activity on the platform. Most social media platforms and apps will store and process your information outside of Canada. We recommend using providers and apps that store your data in jurisdictions that have privacy protection laws equal to Canada's.



Communications Security Establishment
Centre de la sécurité des télécommunications

Ca

Divulgé en vertu de la loi LAI - renseignements non classifiés

BLANK PAGE

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

From: Hatfield, Adam J.
Sent: July-12-19 11:43 AM
To: Mullen, Michèle S;
Cc:
Subject: FW: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat
Attachments: image001.gif; image002.png; image003.png

Classification: UNCLASSIFIED//OFFICIAL USE ONLY

For reference, below is the IT Security Alert sent by the House of Commons team to MPs.

Adam

From:
Sent: July-12-19 11:17 AM
To: Hatfield, Adam J.
Subject: FW: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat

Classification: UNCLASSIFIED//OFFICIAL USE ONLY

Hi Adam,

Here is the message that was sent in case you need to reference....

From:
Sent: July-12-19 10:52 AM
To:
Cc: Belzile, Eric J.
Subject: FW: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat

Hi

The HoC message, as requested on the high side.

Thanks!

From:
Sent: Friday, July 12, 2019 10:51 AM

Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

To:
Subject: Fw: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat

Sent from my BlackBerry 10 smartphone on the Bell network.

From:
Sent: Friday, July 12, 2019 10:43 AM
To:
Subject: Fwd: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat

Begin forwarded message:

From:
Date: July 5, 2019 at 2:06:16 PM EDT
To:
Subject: Fwd: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat

FYI

House of Commons CANADA
Chambre des communes CANADA

From: News/Nouvelles: IT Security/Sécurité des TI <cmqitsec@parl.gc.ca>
Sent: Thursday, July 4, 2019 6:06 PM
To: IT Service Desk/Centre de services des TI
Subject: IT Security Alert – Risks with the WeChat application / Bulletin de sécurité des TI – Les risques liés à l'application WeChat

[cid:image002.gif@01D2342D.CDFD06D0]

[Alert-e]

IT Security Alert – Risks with the WeChat application

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Need assistance?

The IT Service Desk is available to provide assistance 24 hours a day, seven days a week and can be contacted by telephone at 613-947-4774 in Ottawa or toll-free at 1-888-443-4774 or by email at itsd-csti@parl.gc.ca<mailto:issi@parl.gc.ca>.

Note: Please do not reply to this email, as this mailbox is not monitored.

DSRP Cybersecurity team

[Alerte--f]

Bulletin de sécurité des TI – Les risques liés à l'application WeChat

Besoin d'aide ?
Vous pouvez joindre le Centre de services des TI 24 heures par jour, sept jours par semaine par téléphone au 613-947-4774à Ottawa ou sans frais au 1-888-443-4774 ou par courrielà itsd-csti@parl.gc.ca<mailto:itsd-csti@parl.gc.ca>.

NB : Ne répondez pas à ce message, car nous n'assurons aucun suivi de cette boîte de courriels.

L'équipe de la cybersécurité desSNBI

IMPORTANT – FOR RECIPIENTS IN EXTERNAL DEPARTMENTS / AGENCIES:

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

This document is the property of the originating agency and has been provided for your INTERNAL USE ONLY. The originating agency must be consulted prior to further dissemination, in whole or in part, or any disclosure under the ATIA or PA.

IMPORTANT – POUR LES DESTINATAIRES AU SEIN DE MINISTÈRES ET D'ORGANISMES EXTERNES:

Le présent document est la propriété exclusive de l'organisme d'origine et vous a été fourni pour un USAGE INTERNE SEULEMENT. Vous devez consulter l'organisme avant de diffuser le présent document, en tout ou en partie, et avant toute divulgation selon la loi sur l'accès à l'information ou la loi sur la protection des renseignements personnels.

Page 13

is not relevant

est non pertinente

classifiés

BLANK PAGE

Page 15

is not relevant

est non pertinente

BLANK PAGE

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

From: Hatfield, Adam J.
Sent: July-12-19 9:22 AM
To:
Subject: FW: Advice on use of instant messaging / texting services

Classification: UNCLASSIFIED

Hi

Below is what went to PCO last month regarding advice on instant messaging services.

Cheers,
Adam

From: Hatfield, Adam J.
Sent: July-09-19 5:45 PM
To:

Cc: Mullen, Michèle S

Subject: Advice on use of instant messaging / texting services

Classification: UNCLASSIFIED

Hello everyone,

Further to traffic on the high side, this is the advice provided last month to PCO on the use of instant messaging apps and texting services. Attached for interest is a

Thanks,
Adam

++++
USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging services such as Facebook, Twitter, WhatsApp, Skype, and WeChat give you the power to connect with others effortlessly and share information instantly. But using these services can provide threat actors easy access to your information and devices. You can even be placing your online identity and that of your colleagues at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app:

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

* Ensure you're using a service or app from a trustworthy vendor. An app can have a high profile online and be useful, but somewhere there's a company operating that service, accessing your device and holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. Most social media platforms and apps will store and process your information outside of Canada. We recommend using providers and apps that store your data in jurisdictions that have privacy protection laws equal to Canada's.

* Pay close attention to the app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide fast support if your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously.

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

* If you feel you require an app or service but aren't sure of how secure it is, consider having a phone or computer dedicated to that app. Don't use the device for anything else, and never use it for sending sensitive information, even by direct message.
++++

Adam Hatfield
Director of Partnerships / Directeur des Partenariats

CANADIAN CENTRE for CYBER SECURITY | CENTRE CANADIEN pour la CYBERSÉCURITÉ

CANADIAN CENTRE for CYBER SECURITY | CENTRE CANADIEN pour la CYBERSÉCURITÉ

Pages 19 to / à 20

are duplicates

sont des duplicatas

Released under the ATIA - unclassified informati
Divulgé en vertu de la loi LAI - renseignements
classifiés

s.15(1) - DEF

From: Hatfield, Adam J.
Sent: July-05-19 2:15 PM
To: Mullen, Michèle S; Belzile, Eric J.
Subject: FW: Proposed media response re: cybersecurity

Classification: UNCLASSIFIED

From:
Sent: July-05-19 2:11 PM
To: Williams, Christopher R. Jones Scott E. Boucher, Andre J. Hatfield, Adam J. Mclaughlin, Andrew J.
Cc: Media CSEC-CSTC <Media@CSE-CST.GC.CA>
Subject: FW: Proposed media response re: cybersecurity

Classification: UNCLASSIFIED

From: Shank, Stephane <Stephane.Shank@pco-bcp.gc.ca>
Sent: July-05-19 1:51 PM
To: Media CSEC-CSTC <Media@CSE-CST.GC.CA>; 'media-medias@smtp.gc.ca' <media-medias@smtp.gc.ca>; 'Media Relations / Relations avec les médias (PS/SP)' <ps.mediarelations-relationsaveclesmedias.sp@canada.ca>; 'ic.mediarelations-mediasrelations.ic@canada.ca' <ic.mediarelations-mediasrelations.ic@canada.ca>; 'media@international.gc.ca' <media@international.gc.ca>; 'media@justice.gc.ca' <media@justice.gc.ca>
Cc: Tessier, Jean <Jean.Tessier@pco-bcp.gc.ca>; MacKillop, Ken <Ken.MacKillop@pco-bcp.gc.ca>; Diaczuk, Shane <Shane.Diaczuk@pco-bcp.gc.ca>; Nelson, Fiona <Fiona.Nelson@pco-bcp.gc.ca>; ; Mukherjee, Mistu <Mistu.Mukherjee@pco-bcp.gc.ca>; Bujold, Pierre-Alain <Pierre-Alain.Bujold@pco-bcp.gc.ca>; St-Hilaire, Marie-Eve <Marie-Eve.St-Hilaire@pco-bcp.gc.ca>; Binnie, Kate <Kate.Binnie@pco-bcp.gc.ca>; Massabki, Myriam <Myriam.Massabki@pco-bcp.gc.ca>; Donovan, John <John.Donovan@pco-bcp.gc.ca>; Prieur, Cloe <Cloe.Prieur@pco-bcp.gc.ca>; O'Nions, Christine <Christine.O'Nions@pco-bcp.gc.ca>; Doucette, Paul <Paul.Doucette@pco-bcp.gc.ca>; Quenneville, Line <Line.Quenneville@pco-bcp.gc.ca>
Subject: FYI: Proposed media response re: cybersecurity

FYI.

From:
Sent: Friday, July 5, 2019 1:36 PM
To: Shank, Stephane <Stephane.Shank@pco-bcp.gc.ca>
Subject: Proposed media response: cybersecurity

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non classifiés

s.19(1)

Hi Stephane,

Wanted to share this response that we have in approvals with you for your awareness.

Thanks,

NAME OF REPORTER:
CONTACT:
OUTLET:
TOPIC: Cyber security
DATE RECEIVED: July 5, 2019
DEADLINE: July 5, 2019

QUESTION(S) (by phone)

1. Who was the WeChat security alert sent to?
2. Who was it sent from?
3. Was it sent because of a security breach?
4. Was the app commonly used? How commonly used was it?
5. Is this related to the tensions between China and Canada? Is this out of concern of the Chinese law that allows access to company information for intelligence work?

RESPONSE:

The House of Commons' Cybersecurity team issued alerts on the use of WeChat to Members' offices, the House Administration and parliamentary partners on July 4, 2019. Though the application is not in common use, such alerts are sent as standard practice as part of the House Administration's cybersecurity awareness program. Those sent yesterday were issued as a preventative measure. They were not in response to a breach, and there are no other reasons for which the alerts were issued.

While it may be used for personal purposes, WeChat has not been approved by the House of Commons for parliamentary communication. The alerts were sent to remind users to exercise caution in the digital domain.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

From:	Hatfield, Adam J.
Sent:	June-27-19 12:55 PM
To:	
Subject:	FYI: Advice issued this week on use of social media / instant messaging services

Classification: UNCLASSIFIED

Pure FYI – there was back and forth on Tuesday and Wednesday this week with PCO on A&G regarding the use of social media platforms and instant messaging services. Below is what was sent. Comms has this and is giving consideration to webposting either this or a variant of it.

Cheers,
Adam

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging services such as Facebook, Twitter, WhatsApp, Skype, and WeChat give you the power to connect with others effortlessly and share information instantly. But using these services can provide threat actors easy access to your information and devices. You can even be placing your online identity and that of your colleagues at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app:

* Ensure you're using a service or app from a trustworthy vendor. An app can have a high profile online and be useful, but somewhere there's a company operating that service, accessing your device and holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. Most social media platforms and apps will store and process your information outside of Canada. We recommend using providers and apps that store your data in jurisdictions that have privacy protection laws equal to Canada's.

* Pay close attention to the app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide fast support if your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously.

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

* If you feel you require an app or service but aren't sure of how secure it is, consider having a phone or computer dedicated to that app. Don't use the device for anything else, and never use it for sending sensitive information, even by direct message.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements
classifiés

s.15(1) - DEF

From: Hatfield, Adam J.
Sent: June-26-19 4:39 PM
To:
Subject: FW: Wechat

Classification: UNCLASSIFIED

For your awareness. Let's discuss before further dissemination.

Thanks,
Adam

-----Original Message-----
From:
Sent: Wednesday, June 26, 2019 3:22 PM
To: Hatfield, Adam J.
Cc: Belzile, Eric J.
Mullen, Michèle S

Subject: RE: Wechat

This is very helpful, thank you so much Adam. Let's make sure to keep this on our radar when prepping the next security brief to political parties.

Many thanks again,

-----Original Message-----
From: Hatfield, Adam J.
Sent: Wednesday, June 26, 2019 2:34 PM
To:
Cc: Belzile, Eric J.
Mullen, Michèle S

Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi

Below is our advice on this issue, written to be as accessible as possible. Let us know if this meets the need. Sorry for the delay in getting it back to you.

Thanks,
Adam

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging services such as Facebook, Twitter, WhatsApp, Skype, and WeChat give you the power to connect with others effortlessly and share information instantly. But using these services can provide threat actors easy access to your information and devices. You can even be placing your online identity and that of your colleagues at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app:

* Ensure you're using a service or app from a trustworthy vendor. An app can have a high profile online and be useful, but somewhere there's a company operating that service, accessing your device and holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. Most social media platforms and apps will store and process your information outside of Canada. We recommend using providers and apps that store your data in jurisdictions that have privacy protection laws equal to Canada's.

* Pay close attention to the app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide fast support if your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously.

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

* If you feel you require an app or service but aren't sure of how secure it is, consider having a phone or computer dedicated to that app. Don't use the device for anything else, and never use it for sending sensitive information, even by direct message.

-----Original Message-----
From:
Sent: June-26-19 12:52 PM
To: Belzile, Eric J.
Hatfield, Adam J.
Subject: RE: Wechat

Hi there, just wanted to follow up to see if this material is ready to be shared.

Thanks!

Released under the ATIA - unclassified information
Divulgé en vertu de la LAI - renseignements non
classifiés

s.15(1) - DEF

-----Original Message-----
From:
Sent: Tuesday, June 25, 2019 3:05 PM
To: Belzile, Eric J.
Hatfield, Adam J.
Subject: Re: Wechat

Excellent thank you. Hi Adam, if you could share the info by 11:30am tomorrow, we would really appreciate it.

Cheers,

Sent from my BlackBerry 10 smartphone on the Bell network.
Original Message
From:
Sent: Tuesday, June 25, 2019 3:02 PM
To: Belzile, Eric J.; Hatfield, Adam J.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi

We're pulling something together and hope to have it tomorrow. Looping Adam Hatfield in who's team is prim on advice and guidance type issues.

-----Original Message-----
From:
Sent: June-25-19 2:26 PM
To Belzile, Eric J.

Subject: RE: Wechat

Thanks

-----Original Message-----
From:
Sent: Tuesday, June 25, 2019 2:24 PM

To: Belzile, Eric J.

Subject: RE: Wechat

Classification: UNCLASSIFIED

HI

Thanks for the note. I'm synching internally and we'll get back to you.

-----Original Message-----
From:
Sent: June-25-19 2:13 PM
To: Belzile, Eric J.

Subject: RE: Wechat

On this one, PMO is asking for a sense of what kind of advice CSE would provide to MPs on using Wechat.

Please let me know if you will reply to this on the high side.

Thanks,

-----Original Message-----
From:
Sent: Friday, June 21, 2019 4:16 PM
To: Belzile, Eric J.

Subject: RE: Wechat

Classification: UNCLASSIFIED

Thanks
Just heard about this...thought it was a joke. Thanks for flagging.

-----Original Message-----
From:
Sent: June-21-19 8:15 AM
To: Belzile, Eric J.

Subject: Fw: Wechat

Good morning,

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

s.21(1)(a)

Wanted to flag to you that parties are encouraging the use of WeChat in their campaigning. Wondered if this is on your radar and/or will be part of mitigation advise to parties.

Thanks,

Sent from my BlackBerry 10 smartphone on the Bell network.
From:
Sent: Friday, June 21, 2019 8:11 AM
To ;
Cc: Xavier, Caroline
Subject: Wechat

Hi / /

We have been hearing things about MPs being encouraged to download and use Wechat. In some versions of the story it's the and in other variations it's the
This came up at the yesterday. There is clearly room for cse to offer advice to anyone planning to download this, we just have to figure out who is advising this.

- can you please touch base with the HoC for a contact for the - or whatever you think is the best course of action to track this part of the story down.

- we can raise at our 11am meeting to see about the other angle. We should also ensure this is on the agenda for the next Pol Parties meeting.

- can you flag to CCCS in case this is already on their radar.

Thanks.

Sent from my BlackBerry 10 smartphone on the Bell network.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

BLANK PAGE

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non
classifiés

s.15(1) - DEF

From: Jones Scott E.
Sent: June-26-19 3:03 PM
To: Hatfield, Adam J.; Boucher, Andre J.; Belzile, Eric J.
Cc: Mullen, Michèle S; Williams, Christopher R.

Subject: Re: Wechat

Good work.

Scott

From: Hatfield, Adam J.
Sent: Wednesday, June 26, 2019 2:30 PM
To: Boucher, Andre J.; Jones Scott E.; Belzile, Eric J.
Cc: Mullen, Michèle S; Williams, Christopher R.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi folks,

Thanks for the feedback. Below is what I'll be sending back to PCO.

Comms folks, grateful for your guidance on getting a version of this onto a website someplace.

Thanks,

Adam

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging services such as Facebook, Twitter, WhatsApp, Skype, and WeChat give you the power to connect with others effortlessly and share information instantly. But using these services can provide threat actors easy access to your information and devices. You can even be placing your online identity and that of your colleagues at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app:

* Ensure you're using a service or app from a trustworthy vendor. An app can have a high profile online and be useful, but somewhere there's a company operating that service, accessing your device and holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. Most social media platforms and apps will store and process your information outside of Canada. We recommend using providers and apps that store your data in jurisdictions that have privacy protection laws equal to Canada's.

* Pay close attention to the app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide fast support if your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously.

s.15(1) - DEF

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.
* If you feel you require an app or service but aren't sure of how secure it is, consider having a phone or computer dedicated to that app. Don't use the device for anything else, and never use it for sending sensitive information, even by direct message.

From:
Sent: June-26-19 2:15 PM
To: Boucher, Andre J. Hatfield, Adam Jones Scott E. <Scott.Jones@cyber.gc.ca>; Belzile, Eric J.
Cc: Mullen, Michèle S Williams, Christopher R.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi folks,

A couple of general comments. As presented there seems to be an enterprise feel to the style, the best example being that the 'app may provide an entry point into an organization's network'. My sense is these stakeholders are likely using personal devices rather than enterprise provided assets. The bigger risk is to the confidentiality (privacy) of the data on the device, and the device's integrity rather than an organizational network. Perhaps this could be extended a little?

I also think we need to abstract the storage of data element such that risks lie in all facets…….from data on the device, its transit and whatever the app developer does in terms of storage.

Might be splitting hairs…..my opinion.

Thanks,

From:
Sent: June-26-19 1:46 PM
To: Boucher, Andre J. Hatfield, Adam J. Jones Scott E. Belzile, Eric J.
Cc: Mullen, Michèle S ; Williams, Christopher R.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi everyone,

I've made some plain-language edits in-line. Our advice overall is to be more clear about what we're recommending - the current order of the bullets looks more like advice we'd give on cloud storage, so I moved the vendor one to the top. We could also rephrase it to be a list of Dos and Don'ts.

I've added a bullet on the thinking that candidates in certain ridings will argue they must be on specific platforms to reach constituents.

WRT verifying security standards, I recommend deleting that if we aren't going to tell users how to do that. It's not something most people already know.

Happy to discuss if you have any questions.

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

Social media and instant messaging give you the power to connect with others effortlessly and share information instantly. ~~Since these services and apps have become so integrated and integral to daily online activities, many organizations are using them to increase productivity and are allowing employees to use personal social media accounts at work.~~ But using these services can provide threat actors easy and obvious entry points to your organization's networks and information. You can even be placing your online identity and that of your co-workers at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use ~~within your organization~~, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app~~are~~:

* Ensure ~~that~~ you're using a service or app from a trustworthy vendor. An app can have a high profile online, and be useful ~~and functional~~, but somewhere there's a company ~~that is~~ operating that service and ~~that is protecting~~ holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. ~~Generally speaking~~ Most social media platforms and apps will store and process your information outside of Canada. We ~~would~~ recommend ~~that~~ organizations use providers and apps that store your data in jurisdictions that have privacy protection laws ~~in place commensurate with~~ equal to Canada's ~~privacy laws~~.

* Pay close attention to the ~~security functionality that has been built into the~~ app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide clear and fast support if ~~in the event of~~ your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously. ~~If the vendor makes claims about its encryption, verify that relevant standards are met.~~

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

* If you feel you require an app or service but are concerned it isn't secure, consider having a phone dedicated to that app. Don't use the phone for anything else, and never use it for sending sensitive information, even by direct message.

-----Original Message-----
From: Boucher, Andre J.
Sent: June-26-19 12:46 PM
To: Hatfield, Adam J. Jones Scott E. <Scott.Jones@cyber.gc.ca>; Belzile, Eric J.

Cc:
Mullen, Michèle S

Subject: RE: Wechat
Classification: UNCLASSIFIED

Folks - thank you for speedy turnaround!

my quick feedback is that we still need to use more plain language (target a general public audience and vocabulary) and that we should be more specific (perhaps giving examples of actual platforms... when we say "social media" we mean X,Y,Z ...perhaps listing the top 5 used in the world... same with Chat platforms.

The A&G is good. We just need to learn to write in a more accessible way (until all of our readership is Cyber savvy).

Merci
André
André Boucher
Associate Head/ Dirigeant associé
Canadian Centre for Cyber Security/ Centre canadien de cybersécurité
To contact the CCCS/ Pour contacter le CCC:

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

Tel: 1-833-Cyber88
Email/courriel: Contact@cyber.gc.ca
-----Original Message-----
From: Hatfield, Adam J.
Sent: June-26-19 12:23 PM
To: Jones Scott E. <Scott.Jones@cyber.gc.ca>; Boucher, Andre J. Belzile, Eric J.

Cc:

Mullen, Michèle S

Subject: RE: Wechat
Classification: UNCLASSIFIED
Hi everyone,
Apologies for the broadcast email but many have expressed interest in this. Per the emails below, there is a need to provide advice and guidance on selecting social media platforms / instant messaging apps out to political parties (and publicly more generally).
We are proposing the text below, which borrows from existing public guidance (hence the personal tone of the language) but adds elements around country of origin and trust of the vendor. Grateful for all views. Once finalized and approved this will go via email back to PCO, but we will also work with Comms to figure out public posting.
Thanks,
Adam
+++
USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS
Social media and instant messaging give you the power to connect with others effortlessly and share information instantly. Since these services and apps have become so integrated and integral to daily online activities, many organizations are using them to increase productivity and are allowing employees to use personal social media accounts at work. However, when you use these services, you can be providing threat actors easy and obvious entry points to your organization's networks and information. You can even be placing your online identity and that of your co-workers at risk, and exposing your organization's brand and image to harm.
Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use within your organization, you need to consider both the functionality of the service as well as how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app are:
* Think about which nation's laws will apply to your information and your activity on the platform. Generally speaking, most social media platforms and apps will store and process your information outside of Canada. We would recommend that organizations use providers and apps that store your data in jurisdictions that have privacy protection laws in place commensurate with Canada's privacy laws.
* Pay close attention to the security functionality that has been built into the app or platform. Do not use a vendor that does not support strong authentication mechanisms, such as two-factor sign in, and that does not provide clear and fast support in the event of your account being compromised.
* Many services use end-to-end encryption to secure conversations and offer features, like disappearing messages and identity confirmation, to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously. If the vendor makes claims about its encryption, verify that relevant standards are met.
* Ensure that you are using a service or app from a vendor that is trustworthy and reliable. An app can have a high profile online and be useful and functional, but somewhere there is a company that is operating that service and that is protecting your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more and to not use your information for its own purposes.
* Take a moment to consider the sensitivities of your messages before you send them, regardless of your device's security or which app or service you are using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

+++
-----Original Message-----
From:
Sent: June 25, 2019 3:05 PM
To: Belzile, Eric J.
Hatfield, Adam J.
Subject: Re: Wechat
Excellent thank you. Hi Adam, if you could share the info by 11:30am tomorrow, we would really appreciate it.
Cheers,

Sent from my BlackBerry 10 smartphone on the Bell network.
Original Message
From:
Sent: Tuesday, June 25, 2019 3:02 PM
To: Belzile, Eric J.; Hatfield, Adam J.
Subject: RE: Wechat
Classification: UNCLASSIFIED
Hi
We're pulling something together and hope to have it tomorrow. Looping Adam Hatfield in who's team is prim on advice and guidance type issues.

-----Original Message-----
From:
Sent: June-25-19 2:26 PM
To: Belzile, Eric J.

Subject: RE: Wechat
Thanks

-----Original Message-----
From:
Sent: Tuesday, June 25, 2019 2:24 PM
To: Belzile, Eric J.

Subject: RE: Wechat
Classification: UNCLASSIFIED
HI
Thanks for the note. I'm synching internally and we'll get back to you.

-----Original Message-----
From:
Sent: June-25-19 2:13 PM
To: Belzile, Eric J.

Subject: RE: Wechat
On this one, PMO is asking for a sense of what kind of advice CSE would provide to MPs on using Wechat.
Please let me know if you will reply to this on the high side.
Thanks,

s.15(1) - DEF

-----Original Message-----
From:
Sent: Friday, June 21, 2019 4:16 PM
To: Belzile, Eric J.

Subject: RE: Wechat
Classification: UNCLASSIFIED
Thanks
Just heard about this...thought it was a joke. Thanks for flagging.
-----Original Message-----
From:
Sent: June-21-19 8:15 AM
To: Belzile, Eric J.

Subject: Fw: Wechat
Good morning,
Wanted to flag to you that parties are encouraging the use of WeChat in their campaigning. Wondered if this is on your radar and/or will be part of mitigation advise to parties.
Thanks,

Sent from my BlackBerry 10 smartphone on the Bell network.
From:
Sent: Friday, June 21, 2019 8:11 AM
To:
Cc: Xavier, Caroline
Subject: Wechat
Hi
We have been hearing things about MPs being encouraged to download and use Wechat. In some versions of the story it's the and in other variations it's the
This came up at the yesterday. There is clearly room for cse to offer advice to anyone planning to download this, we just have to figure out who is advising this.
- can you please touch base with the HoC for a contact for the - or whatever you think is the best course of action to track this part of the story down.
- we can raise at our 11am meeting to see about the other angle. We should also ensure this is on the agenda for the next Pol Parties meeting.
- can you flag to CCCS in case this is already on their radar.
Thanks.

Sent from my BlackBerry 10 smartphone on the Bell network.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

From: Hatfield, Adam J.
Sent: June-26-19 12:23 PM
To: Jones Scott E.; Boucher, Andre J.; Belzile, Eric J.;
Cc: Mullen, Michèle S;

Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi everyone,

Apologies for the broadcast email but many have expressed interest in this. Per the emails below, there is a need to provide advice and guidance on selecting social media platforms / instant messaging apps out to political parties (and publicly more generally).

We are proposing the text below, which borrows from existing public guidance (hence the personal tone of the language) but adds elements around country of origin and trust of the vendor. Grateful for all views. Once finalized and approved this will go via email back to PCO, but we will also work with Comms to figure out public posting.

Thanks,
Adam

+++

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging give you the power to connect with others effortlessly and share information instantly. Since these services and apps have become so integrated and integral to daily online activities, many organizations are using them to increase productivity and are allowing employees to use personal social media accounts at work. However, when you use these services, you can be providing threat actors easy and obvious entry points to your organization's networks and information. You can even be placing your online identity and that of your co-workers at risk, and exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use within your organization, you need to consider both the functionality of the service as well as how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app are:

* Think about which nation's laws will apply to your information and your activity on the platform. Generally speaking, most social media platforms and apps will store and process your information outside of Canada. We would recommend that organizations use providers and apps that store your data in jurisdictions that have privacy protection laws in place commensurate with Canada's privacy laws.

* Pay close attention to the security functionality that has been built into the app or platform. Do not use a vendor that does not support strong authentication mechanisms, such as two-factor sign in, and that does not provide clear and fast support in the event of your account being compromised.

Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

* Many services use end-to-end encryption to secure conversations and offer features, like disappearing messages and identity confirmation, to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously. If the vendor makes claims about its encryption, verify that relevant standards are met.

* Ensure that you are using a service or app from a vendor that is trustworthy and reliable. An app can have a high profile online and be useful and functional, but somewhere there is a company that is operating that service and that is protecting your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more and to not use your information for its own purposes.

* Take a moment to consider the sensitivities of your messages before you send them, regardless of your device's security or which app or service you are using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

+++
-----Original Message-----
From:
Sent: June 25, 2019 3:05 PM
To: Belzile, Eric J.
Hatfield, Adam J.
Subject: Re: Wechat

Excellent thank you. Hi Adam, if you could share the info by 11:30am tomorrow, we would really appreciate it.

Cheers,

Sent from my BlackBerry 10 smartphone on the Bell network.
Original Message
From:
Sent: Tuesday, June 25, 2019 3:02 PM
To: | Belzile, Eric J.; Hatfield, Adam J.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi

We're pulling something together and hope to have it tomorrow. Looping Adam Hatfield in who's team is prim on advice and guidance type issues.

-----Original Message-----
From:
Sent: June-25-19 2:26 PM
To: Belzile, Eric J.

Subject: RE: Wechat

Released under the ATIA - unclassified informatio
Divulgé en vertu de la loi LAI - renseignements n
classifiés

s.15(1) - DEF

Thanks

-----Original Message-----
From:
Sent: Tuesday, June 25, 2019 2:24 PM
To: Belzile, Eric J.

Subject: RE: Wechat

Classification: UNCLASSIFIED

HI

Thanks for the note. I'm synching internally and we'll get back to you.

-----Original Message-----
From:
Sent: June-25-19 2:13 PM
To: Belzile, Eric J.

Subject: RE: Wechat

On this one, PMO is asking for a sense of what kind of advice CSE would provide to MPs on using Wechat.

Please let me know if you will reply to this on the high side.

Thanks,

-----Original Message-----
From:
Sent: Friday, June 21, 2019 4:16 PM
To: Belzile, Eric J.

Subject: RE: Wechat

Classification: UNCLASSIFIED

Thanks
Just heard about this...thought it was a joke. Thanks for flagging.

Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

s.21(1)(a)

-----Original Message-----
From:
Sent: June-21-19 8:15 AM
To: Belzile, Eric J.

Subject: Fw: Wechat

Good morning,

Wanted to flag to you that parties are encouraging the use of WeChat in their campaigning. Wondered if this is on your radar and/or will be part of mitigation advise to parties.

Thanks,

Sent from my BlackBerry 10 smartphone on the Bell network.
From:
Sent: Fridav, June 21. 2019 8:11 AM
To:
Cc: Xavier, Caroline
Subject: Wechat

Hi

We have been hearing things about MPs being encouraged to download and use Wechat. In some versions of the story it's the and in other variations it's the
This came up at the yesterday. There is clearly room for cse to offer advice to anyone planning to download this, we just have to figure out who is advising this.

- can you please touch base with the HoC for a contact for the - or whatever you think is the best course of action to track this part of the story down.

- we can raise at our 11am meeting to see about the other angle. We should also ensure this is on the agenda for the next Pol Parties meeting.

can you flag to CCCS in case this is already on their radar.

Thanks.

Sent from my BlackBerry 10 smartphone on the Bell network.

Pages 41 to / à 62

are not relevant

sont non pertinentes

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF
s.21(1)(b)

From:
Sent: July-11-19 8:35 AM
To: Foreman, Ryan
Cc:
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hi Ryan,

To be direct,

However, WeChat is not the same as Facebook Messenger or WhatsApp for example.

From:
Sent: July-11-19 5:54 AM
To: Foreman, Ryan

Cc:
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hi Ryan, our product is not specific to GC personnel it encompasses everyone.

Thanks,

From: Foreman, Ryan
Sent: July-10-19 12:52 PM

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

s.21(1)(a)

To:
Cc:

Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Thanks

(On a break from a day long training session). Sounds like the product that mentioned is going to be a separate product specifically for GC personnel on the use of WeChat with much stronger security messaging? In our comms product we were careful to mention service providers but not single any particular one out. We should have a final version for approvals later today or tomorrow.

Ryan

From:
Sent: July-09-19 4:21 PM
To: Foreman, Ryan
Cc:

Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Thanks, Ryan,

The overall thrust of this guidance is fine (making sure the application is hosted and developed in countries with similar privacy and security outlook as Canada is especially helpful).

<< File: proof-v03-1920-0624-cyber-centre-social-media-chat-apps-e.pdf >>

From: Foreman, Ryan
Sent: July-09-19 1:08 PM
To:
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF
s.21(1)(a)

Sure – here's the draft publication that will be posted on the Cyber Centre web site. There are a few more changes in progress to the document.

Ryan

<< File: proof-v03-1920-0624-cyber-centre-social-media-chat-apps-e.pdf >>

From:
Sent: July-09-19 11:32 AM
To: Foreman, Ryan
Subject: RE: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hey Ryan;

May I take a look at your communication related to WeChat?

From:
Sent: July-09-19 11:29 AM
To:
Foreman, Ryan

Subject: WeChat Inquiry

Classification: CONFIDENTIAL//CANADIAN EYES ONLY

Hi

In the discussion this morning, you had asked if CSE currently has any official Advice and Guidance (A&G) regarding WeChat.

I understand that Ryan's group has some generic A&G,

Is SITE asking for something more official?

At present,

Foreign use of this product should be limited to unclassified data only. CSE does not specify how WeChat should be used in individual counties as this more in the mandate of GAC.

We can dig into this one more if required.

Thanks

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

Pages 67 to / à 70

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

Hatfield, Adam J.

From: Hatfield, Adam J.
Sent: June-26-19 4:56 PM
To: [redacted]
Cc: Mullen, Michèle S; [redacted]
Subject: RE: Wechat

Classification: PROTECTED B

Hi [redacted]

Thanks for the comments. The email went off to PCO and people seemed okay with it as an email, so I would consider that closed.

However, I was speaking to [redacted] afterwards about if/how we get some of this material online publicly, and if so, do we take a close second look at the advice. In that context, your comments are still timely. Please forward them to her (I can't seem to reach her PKI key from here) for consideration.

Thanks,
Adam

From: [redacted]
Sent: Wednesday, June 26, 2019 3:19 PM
To: Hatfield, Adam J. [redacted]
Cc: Mullen, Michèle S [redacted]
Subject: RE: Wechat

Classification: PROTECTED B

Adam

Sending a few comments your way to avoid an email storm and FYC. It may be too late based on Scott's well done email ☹. Need to be faster on the trigger.

Comments below in Red

[redacted]

From: Hatfield, Adam J. [redacted]
Sent: June-26-19 2:31 PM
To: [redacted] Boucher, Andre J. [redacted] Jones Scott E. <Scott.Jones@cyber.gc.ca>; Belzile, Eric J. [redacted]
Cc: [redacted]
Mullen, Michèle S [redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

[redacted]

[redacted] Williams, Christopher R. [redacted]

Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi folks,

Thanks for the feedback. Below is what I'll be sending back to PCO.

Comms folks, grateful for your guidance on getting a version of this onto a website someplace.

Thanks,
Adam

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging services such as Facebook, Twitter, WhatsApp, Skype, and WeChat give you the power to connect with others effortlessly and share information instantly. But using these services can provide threat actors easy access to your information and devices. You can even be placing your online identity and that of your colleagues at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app:

* Ensure you're using a service or app from a trustworthy vendor. An app can have a high profile online and be useful, but somewhere there's a company operating that service, accessing your device and holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. Most social media platforms and apps will store and process your information outside of Canada. We recommend using providers and apps that store your data in jurisdictions that have privacy protection laws equal to Canada's.

Ask yourself whether you trust it not to use your information for its own purposes. It is their business model so the likelihood it will not be used for its own purposes is very small. If you are using a "free" social media service, it is using your information for its own purposes (which is using your information to target you with advertising for profit or selling it to others), so I'm not sure what point we are trying to make here.

* Pay close attention to the app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide fast support if your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously.

These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously which is a good point. Again, this is true in terms about protecting your information from other parties, but as the $5B fine the EU and the FTC are considering against FaceBook would indicate, they do not protect against the provider itself bypassing all of those mechanisms to access your data. We have also removed the only reference we had to a publication that is actually talking to the cryptographic mechanisms used, but I understand Andre's point that this needs to be kept simple for the intended audience.

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

* If you feel you require an app or service but aren't sure of how secure it is, consider having a phone or computer dedicated to that app. Don't use the device for anything else, and never use it for sending sensitive information, even by direct message.

It was good for [redacted] to include this ([redacted] I'm not sure how well received this would be by an individual, but it is the best advice we have to offer.

[redacted]

From: [redacted]
Sent: June-26-19 2:15 PM
To: [redacted] Boucher, Andre J. [redacted] Hatfield, Adam J. [redacted] Jones Scott E. <Scott.Jones@cyber.gc.ca>; Belzile, Eric J. [redacted]
Cc: [redacted] Mullen, Michèle S [redacted] Williams, Christopher R. [redacted]
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi folks,

A couple of general comments. As presented there seems to be an enterprise feel to the style, the best example being that the 'app may provide an entry point into an organization's network'. My sense is these stakeholders are likely using personal devices rather than enterprise provided assets. The bigger risk is to the confidentiality (privacy) of the data on the device, and the device's integrity rather than an organizational network. Perhaps this could be extended a little?

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

I also think we need to abstract the storage of data element such that risks lie in all facets…….from data on the device, its transit and whatever the app developer does in terms of storage.

Might be splitting hairs…..my opinion.

Thanks,

[redacted]

From: [redacted]
Sent: June-26-19 1:46 PM
To: Boucher, Andre J. [redacted] Hatfield, Adam J. [redacted] Jones Scott E. <Scott.Jones@cyber.gc.ca>; Belzile, Eric J. [redacted]
Cc: [redacted] Mullen, Michèle S [redacted] Williams, Christopher R.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi everyone,

I've made some plain-language edits in-line. Our advice overall is to be more clear about what we're recommending - the current order of the bullets looks more like advice we'd give on cloud storage, so I moved the vendor one to the top. We could also rephrase it to be a list of Dos and Don'ts.

I've added a bullet on the thinking that candidates in certain ridings will argue they must be on specific platforms to reach constituents.

WRT verifying security standards, I recommend deleting that if we aren't going to tell users how to do that. It's not something most people already know.

Happy to discuss if you have any questions.

[redacted]

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging give you the power to connect with others effortlessly and share information instantly. ~~Since these services and apps have become so integrated and integral to daily online activities, many organizations are using them to increase productivity and are allowing employees to use personal social media accounts at work.~~ But using these services can provide threat actors easy and obvious

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

entry points to your organization's networks and information. You can even be placing your online identity and that of your co-workers at risk, or exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use ~~within your organization~~, you need to consider both the functionality of the service and how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app~~are~~:

* Ensure ~~that~~ you're using a service or app from a trustworthy vendor. An app can have a high profile online, and be useful ~~and functional~~, but somewhere there's a company ~~that is~~ operating that service and ~~that is protecting~~ holding your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more. Ask yourself whether you trust it not to use your information for its own purposes.

* Think about which nation's laws will apply to your information and your activity on the platform. ~~Generally speaking~~ Most social media platforms and apps will store and process your information outside of Canada. We ~~would~~ recommend ~~that~~ organizations use providers and apps that store your data in jurisdictions that have privacy protection laws ~~in place commensurate with~~ equal to Canada's ~~privacy laws~~.

* Pay close attention to the ~~security functionality that has been built into the~~ app or platform's security functions. Don't use a vendor that doesn't support strong authentication mechanisms, such as two-factor sign in, and that doesn't provide clear and fast support if ~~in the event of~~ your account is compromised.

* Many services use end-to-end encryption to secure conversations, and offer features like disappearing messages and identity confirmation to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously. ~~If the vendor makes claims about its encryption, verify that relevant standards are met.~~

* Take a moment to consider the sensitivity of your messages before you send them, regardless of your device's security or which app or service you're using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

* If you feel you require an app or service but are concerned it isn't secure, consider having a phone dedicated to that app. Don't use the phone for anything else, and never use it for sending sensitive information, even by direct message.

-----Original Message-----
From: Boucher, Andre J. [redacted]
Sent: June-26-19 12:46 PM
To: Hatfield, Adam J. [redacted] Jones Scott E. <Scott.Jones@cyber.gc.ca>; Belzile, Eric J. [redacted]
Cc: [redacted] Mullen, Michèle S [redacted]

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

[redacted]

Subject: RE: Wechat

Classification: UNCLASSIFIED

Folks - thank you for speedy turnaround!

my quick feedback is that we still need to use more plain language (target a general public audience and vocabulary) and that we should be more specific (perhaps giving examples of actual platforms... when we say "social media" we mean X,Y,Z ...perhaps listing the top 5 used in the world... same with Chat platforms.

The A&G is good. We just need to learn to write in a more accessible way (until all of our readership is Cyber savvy).

Merci
André

André Boucher
Associate Head/ Dirigeant associé
Canadian Centre for Cyber Security/ Centre canadien de cybersécurité

To contact the CCCS/ Pour contacter le CCC:
Tel: 1-833-Cyber88
Email/courriel: Contact@cyber.gc.ca

-----Original Message-----
From: Hatfield, Adam J. [redacted]
Sent: June-26-19 12:23 PM
To: Jones Scott E. <Scott.Jones@cyber.gc.ca>; Boucher, Andre J. [redacted] Belzile, Eric J. [redacted]
Cc: [redacted] Mullen, Michèle S [redacted]

[redacted]

Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi everyone,

Apologies for the broadcast email but many have expressed interest in this. Per the emails below, there is a need to provide advice and guidance on selecting social media platforms / instant messaging apps out to political parties (and publicly more generally).

We are proposing the text below, which borrows from existing public guidance (hence the personal tone of the language) but adds elements around country of origin and trust of the vendor. Grateful for all

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

views. Once finalized and approved this will go via email back to PCO, but we will also work with Comms to figure out public posting.

Thanks,
Adam

+++

USE OF SOCIAL MEDIA, INSTANT MESSAGING, AND TEXTING PLATFORMS AND APPS

Social media and instant messaging give you the power to connect with others effortlessly and share information instantly. Since these services and apps have become so integrated and integral to daily online activities, many organizations are using them to increase productivity and are allowing employees to use personal social media accounts at work. However, when you use these services, you can be providing threat actors easy and obvious entry points to your organization's networks and information. You can even be placing your online identity and that of your co-workers at risk, and exposing your organization's brand and image to harm.

Instant messaging apps and social media platforms are not all created equal. In deciding what tools to use within your organization, you need to consider both the functionality of the service as well as how secure and private your information and activity will be. Some factors to consider in assessing the risks of using a particular service or app are:

* Think about which nation's laws will apply to your information and your activity on the platform. Generally speaking, most social media platforms and apps will store and process your information outside of Canada. We would recommend that organizations use providers and apps that store your data in jurisdictions that have privacy protection laws in place commensurate with Canada's privacy laws.

* Pay close attention to the security functionality that has been built into the app or platform. Do not use a vendor that does not support strong authentication mechanisms, such as two-factor sign in, and that does not provide clear and fast support in the event of your account being compromised.

* Many services use end-to-end encryption to secure conversations and offer features, like disappearing messages and identity confirmation, to help promote confidentiality. These are not foolproof - an untrustworthy recipient can still take a screenshot of a conversation and post it online – but they are an indication the provider takes security seriously. If the vendor makes claims about its encryption, verify that relevant standards are met.

* Ensure that you are using a service or app from a vendor that is trustworthy and reliable. An app can have a high profile online and be useful and functional, but somewhere there is a company that is operating that service and that is protecting your information. You need to decide if you trust the vendor to provide an application that does what it claims and nothing more and to not use your information for its own purposes.

* Take a moment to consider the sensitivities of your messages before you send them, regardless of your device's security or which app or service you are using. If the information is highly sensitive, you need to be sure you can trust the vendor of the service you are using.

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

+++
-----Original Message-----
From: [redacted]
Sent: June 25, 2019 3:05 PM
To: [redacted] Belzile, Eric J. [redacted] Hatfield, Adam J. [redacted]
Subject: Re: Wechat

Excellent thank you. Hi Adam, if you could share the info by 11:30am tomorrow, we would really appreciate it.

Cheers,

[redacted]

Sent from my BlackBerry 10 smartphone on the Bell network.
Original Message
From: [redacted]
Sent: Tuesday, June 25, 2019 3:02 PM
To: [redacted] [redacted] Belzile, Eric J.; Hatfield, Adam J.
Subject: RE: Wechat

Classification: UNCLASSIFIED

Hi [redacted]

We're pulling something together and hope to have it tomorrow. Looping Adam Hatfield in who's team is prim on advice and guidance type issues.

[redacted]

-----Original Message-----
From: [redacted]
Sent: June-25-19 2:26 PM
To: [redacted] Belzile, Eric J. [redacted]
Subject: RE: Wechat

Thanks [redacted]

[redacted]

-----Original Message-----
From: [redacted]
Sent: Tuesday, June 25, 2019 2:24 PM

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

To: [redacted] [redacted] Belzile, Eric J. [redacted]
Subject: RE: Wechat

Classification: UNCLASSIFIED

HI [redacted]

Thanks for the note. I'm synching internally and we'll get back to you.

[redacted]

-----Original Message-----
From: [redacted]
Sent: June-25-19 2:13 PM
To: [redacted] Belzile, Eric J.
[redacted]
Subject: RE: Wechat

On this one, PMO is asking for a sense of what kind of advice CSE would provide to MPs on using Wechat.

Please let me know if you will reply to this on the high side.

Thanks,

[redacted]

-----Original Message-----
From: [redacted]
Sent: Friday, June 21, 2019 4:16 PM
To: [redacted] [redacted] Belzile, Eric J. [redacted]
Subject: RE: Wechat

Classification: UNCLASSIFIED

Thanks [redacted]
Just heard about this...thought it was a joke. Thanks for flagging.

-----Original Message-----
From: [redacted]
Sent: June-21-19 8:15 AM
To: [redacted] Belzile, Eric J. [redacted]
[redacted]
Subject: Fw: Wechat

Released under the ATIA - unclassified information
Divulgé en vertu de la loi LAI - renseignements non classifiés

s.15(1) - DEF

s.21(1)(a)

Good morning,

Wanted to flag to you that parties are encouraging the use of WeChat in their campaigning. Wondered if this is on your radar and/or will be part of mitigation advise to parties.

Thanks,

[redacted]

Sent from my BlackBerry 10 smartphone on the Bell network.
From: [redacted]
Sent: Friday, June 21, 2019 8:11 AM
To: [redacted]
Cc: Xavier, Caroline
Subject: Wechat

Hi [redacted] / [redacted] / [redacted]

We have been hearing things about MPs being encouraged to download and use Wechat. In some versions of the story it's the [redacted] and in other variations it's the [redacted]
This came up at the [redacted] yesterday. There is clearly room for cse to offer advice to anyone planning to download this, we just have to figure out who is advising this.

[redacted] can you please touch base with the HoC for a contact for the [redacted] - or whatever you think is the best course of action to track this part of the story down.

[redacted] - we can raise at our 11am meeting to see about the other angle. We should also ensure this is on the agenda for the next Pol Parties meeting.

[redacted] can you flag to CCCS in case this is already on their radar.

Thanks.

[redacted]

Sent from my BlackBerry 10 smartphone on the Bell network.