Safe Support

A Digital Digest for the Ontario Coalition of Rape Crisis Centres
Winter 2023

Tech Safety and Security: Common issues for GBV organizations

Impersonation

With text, chat and messaging, it's hard to tell if the person you're communicating with is really who they say they are.

Abusive people impersonate support seekers in order to harass GBV workers or to get access to a support seeker's information.

Prepare for the inevitable

- Adapt crisis line and email policies and procedures to guide chat, text and messaging support services.

- Set safe words and safety plan with support seekers so you can identify them and know what to do if they are being impersonated.

- Don't discuss previous exchanges with support seekers. Let them know this is your policy.

- Encourage support seekers to delete your exchanges.
    - **Safe Support Chat** (https://www.safesupport.chat) deletes all chat exchanges as soon as they end.

Dealing with abusive people

It's not unusual for our organizations to receive abusive messages through chat, text, social media and email.

When you receive an abusive message:

- Save it or take a screen shot, noting the time and date.

- Do not engage with the sender.

- Connect with your supervisor and make time for self care.

Use the screen shot with your team to prepare for these situations in the future.

Determine:

- How to support one another when your organization is targeted
- What to do if a staff member becomes the focus of the abuse
- When to contact police

Keep the screen shot in order to monitor abuse and identify changes and escalations. You can use screen shots as evidence.

Here's how to

- Take a screen shot (https://www.wikihow.com/Take-a-Screen-Shot-(Screen-Capture))
- Manage digital evidence (https://bcsth.ca/digitalevidencetoolkit/how-to-back-up-and-store-evidence-of-technology-facilitated-violence/)

Super tip: Don't use personal devices!

The use of the organization's devices

- Creates a layer of protection for staff when dealing with abuse
- Improves the management and privacy of support seekers' information

Assessing new tech

What to find out

When integrating a new product into your services, the proper management of support seekers' information needs to be a priority.

Here are ways to learn how committed a technology is to the security of your data:

- Search the name of the product and "data breach"
- Look for privacy setting information and tips on its website

- Read the privacy policy
    - Is it easy to read?
    - What data is collected?
    - Who has access to it?
    - Where is it stored?
    - How long is it stored?
    - Is it encrypted? If so, who has the "key"?

Safe Support Chat (https://www.safesupport.chat) does not keep a record of any data from exchanges with support seekers.

What to avoid

These requirements collect a lot of data:

- Everyone must have an account in order to use the product
- To use it, the product must be downloaded
- Users are encouraged to log into the product through their Facebook or Google account

The "free" version of a product is a great way to test features, but you are paying for free access with user data. This data will be sold.

For more tips on integrating new tech services, see Emerging Stronger: Promising Practices in Virtual Service Delivery from the Ontario Association of Interval and Transition Houses (OAITH).

Phishing Scams

What it is

- **Phishing:** A malicious attempt, usually by email or text, to get sensitive information or to get someone to download malware
- **Spoofing:** The person sending the phishing message impersonates one of your contacts or a well known company or institution (e.g. bank, CRA)

See examples of phishing (https://www.tessian.com/blog/what-does-a-spear-phishing-email-look-like/)

What to watch for

- In an email, the display name and email address are different and the domain is fake (e.g. FedEx.Net, CRA.com).

- The text or email message will be urgent and will include a link: don't click the link!

If you click the link

- Let your supervisor/team/IT know immediately
- Change passwords for all accounts
- Report the scam to the Canadian Anti-Fraud Centre

The Safe Support Digital Digest is another component of the OCRCC's **Preventing Gender-Based Violence Program - Using Technology to Better Support Survivors in Frontline Settings**, funded by Ministry of Children, Community and Social Services, Office of Women's Issues, Ontario.

This digest is created by Paula Wansbrough for PRIMAL GLOW Communications.