Tech Safety Bingo!

A fun way to explore tech safety issues with support seekers or work colleagues

Accurate as of January 2023

This resource 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, and was created by Kim Allen and Paula Wansbrough of PRIMAL GLOW Communications.

Preparation

- If using this game with support seekers
    - Recognize that some items in the squares in this game might trigger a person if they've suffered online abuse. You might decide to change or skip some the items.
    - Conducting this game with a co-facilitator is a good idea in case a participant needs support.
- Familiarize yourself with the information about each item below. Keep in mind that tech changes quickly, so information may no longer be accurate and links may have changed.
- Decide when participants can mark a square on their card:
    - Any time you read out a new item? (i.e. every time: everyone/no one wins)
      or
    - When participants are familiar with a term or think an action makes sense? (i.e. most times: most people win based on knowledge not actions)
      or
    - Only when participants know a term or regularly do the action?
- Provide each participant with a bingo card.
    - If this will be an in-person event, print out the cards ahead of time.
    - If you are doing this virtually, send participants the cards as a PDF ahead of time and ask them to print them out, or mail the participants the printed cards.
- Ensure participants have a way to mark the card, either with coins or dried beans to place on squares, or a pen/pencil to mark squares.
- Print a card, cut out the squares and put the squares into a container so that you can randomly select items to read out.
    - However, depending on your audience and your goals for the activity, you may want to be more purposeful in the items you select to read out.

Instructions

- The game leader selects a square and reads out the item.
- The game leader will share the information associated with the item (see below) and might encourage suggestions, comments and experiences from participants.

- Participants mark the item's square on their card (depending on the strategy you've chosen, e.g. every time you read out an item or only when they are familiar with the item).
- When someone has marked all items in a row, they call out "Bingo!"
    - The game leader may wish to ask the participant to read out their row of actions and talk about each item in their row.
- The game can end when someone finishes a row, or you might want to continue going through all the items on the card.
- You might wish to wrap up the game reminding participants that they have every right to use social media and other online apps and platforms. Visit https://TakeBackTheTech.net/ for inspiration.

Under the "B"

- Spoofing
    - Do you know what spoofing is? If so, mark the spot on the card.
    - Spoofing is impersonation used to gain a person's trust.
    - Spoofing is often used in email scams. A malicious party will pretend to be a trusted source, such as a well-known business or someone the email recipient knows, in order to trick the recipient into providing sensitive information or clicking a link that will result in the download of malware.
- Geolocation
    - Do you know how to turn off geolocation for your camera and apps? If so, mark the spot on the card.
    - Every picture you take will contain information telling where it was taken unless you turn off the geolocation in your phone's privacy settings. This information is visible to anyone who can view the photo online. Keep this in mind when posting images of yourself and others on social media.
    - Apps often track your location, whether this is necessary or not for their function; it's a way they gather data about their users. You can turn this option off.
    - You can set some apps to only track your location when you're using the app, which is handy for map-related apps.
    - Turning off the geolocation for your phone will mean: 1) 911 will not be able to locate you if you call, and 2) you will not be able to find your phone if you lose it (and others will not be able to find you with your phone).
- Manage email
    - Mark this off if you know some ways to manage email with an abusive person.
    - If you must communicate with an abusive person, email is a good strategy because 1) it creates a record that you can sort through fairly easily; and 2) you'll respond a little slower than you might with text.

- If you must deal with an abusive person fairly often, create a separate email account and schedule times to check it. When the person contacts you, take time to compose your response. Always make your response in a new email to avoid creating an email thread, the text of which can be easily changed.
- Other tips are available: https://familycourtandbeyond.ca/keep-safe/web-phone-safety/managing-electronic-communication-with-an-abusive-ex-partner/

- Save evidence of tech abuse
  - Do you know how to save evidence of tech abuse? If you know how to do a "screen capture" or "screen shot", you do. If so, mark the spot on the card.
  - If you don't know how, search for "how to take a screen shot" or visit: https://www.wikihow.com/Take-a-Screen-Shot-(Screen-Capture)
  - If someone has posted something abusive about you or an intimate image, take a screen shot. Be sure to include the website address, and if visible, the author and time of posting.
  - Here are tips on how to manage your digital evidence: https://bcsth.ca/digitalevidencetoolkit/best-practices-for-collecting-digital-evidence-of-technology-facilitated-violence/
- Online violence is often illegal
  - If you knew this, mark the spot on the card.
  - These online abuse tactics are against the law in Canada.
    - Sharing intimate photos of someone without their consent
    - Stalking
    - Intimidation
    - Blackmail
    - Child pornography
  - To learn more about this, visit: https://bcsth.ca/techsafetytoolkit/ Scroll to the Legal Remedies section.

Under the "I"

- Phone is locked
  - If your phone is locked, mark this square.
  - To learn how to lock your phone, search for "lock my [type of phone, e.g. iPhone, Android]". Usually the option is available under the privacy settings.
  - Locking your phone protects your privacy if someone accesses your phone, such as if you were to lose it or someone wants to monitor your online activities.
  - If you are concerned that someone has been snooping on your phone (like a partner or relative) and you want to lock it, think about what may happen if they can no longer access it. You may want to create a safety plan.
- A variety of profile pictures
  - If you use different profile pictures in your accounts, mark the spot.
  - Malicious people use searches of profile pictures to learn about a person they are targeting and for identity theft purposes. A variety of profiles images will

limit someone from finding you in all the platforms you use (e.g. social media, dating sites, work, school and volunteer sites).
    - If you are concerned about online privacy, avoid using a clear image of your face as your profile image. Sunglasses, hats and hair are helpful. Your friends will know it's you. Or use an image of scenery or a drawing.
- Doxxing
    - If you know what doxxing is, mark this spot.
    - Doxxing is when a person or a group of people share personal information about another person online with the intent of causing harm.
    - This might include publicizing a person's home address, contact information, names of their family members and their former identity and personal history, intimate and/or manipulated photos.
    - Doxxing is a common gender-abuse tactic used against ex-partners or people who take a stand on a particular issue. If you are doxxed or feel you may be targeted, the Electronic Frontier Foundation provides tips on keeping safer: https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-how-minimize-harm
    - If you see doxing happening, you can help: https://iheartmob.org/pages/bystander-intervention-online
- Video chat before you meet
    - If this makes sense to you, mark this spot.
    - Meeting a new person in-person for the first time? Take care. Sometimes people you connect with online aren't who they say they are.
    - Other tips:
        - Check the person out on social media.
        - Search for their image online.
        - Let a reliable friend know who you're meeting and where you're going. Keep in touch with your friend throughout your meet-up with the new person.
        - Meet in a public place.
        - Plan your transportation home ahead of time.
- Change your passwords regularly
    - If you change your passwords at least once or twice a year, mark this spot.
    - If not, put yourself on a seasonal schedule. Every 4 months change important passwords like your email, social media and any sites with financial information, like banking and where you buy apps.
    - Use long passphrases that mix upper and lower case letters, numbers and symbols. Come up with ones that make you smile every time you type them: 1L0v3Ch0c0l@t3! or L1ke@f1shNeeds@B1ke
    - See a list of the most common passwords on Wikipedia, which you should never use: https://en.wikipedia.org/wiki/List_of_the_most_common_passwords and get tips on managing your passwords: https://www.hivesystems.io/blog/are-your-passwords-in-the-green-2020

Under the "N"

- Don't share passwords
    - If you don't share any of your passwords with anyone else, mark this spot.
    - It's tempting to share your passwords with people close to you. However, to keep safe and secure, try not to. No one should ever push you to share your passwords.
    - Having access to other people's passwords also makes you vulnerable if anything goes wrong related to those accounts. If someone wants to share their passwords with you, find a way to kindly refuse.
- Log out of accounts
    - If you usually log out of all your app accounts (like email, Instagram, etc.), mark this spot.
    - Logging out is especially important if you don't lock your device.
    - Some accounts, like online banking accounts, will automatically close after a short period of inactivity. This is to protect your privacy. But most don't.
    - When you leave an account open, like WhatsApp, anyone who can access your device – maybe you are using a public computer, or someone knows the password for your phone -- will be able to access the account.
- Online abuse is real abuse
    - If you think this statement is true, mark the spot.
    - Some people still believe that online abuse isn't "real" abuse. Anyone who's been attacked online will know it can be as scary, upsetting and maddening as other forms of violence.
- 2-factor authentication
    - If you use 2-factor authentication, mark this spot.
    - 2-factor or 2-step or multi-factor authentication is a form of password protection. When you use a 2-factor authentication tool, in order to log into an account, you have to input two passwords each from a different device or program. While it means it takes a bit longer to get into the account, it's like having two locks on the door.
- Spyware
    - If you know what spyware is, mark this spot.
    - Spyware is an application an abusive person installs on someone's phone or laptop or other device in order to spy on them. The program will let the abusive person see everything that happens on the device: location, messages, passwords, photos, etc.
    - Sometimes spyware is installed through an attachment that is texted or emailed and downloaded. Sometimes the abusive person gets access to the device and installs the spyware manually.
    - It can be very difficult to tell if spyware is installed on a device, although there are some clues. A key clue is if the abusive person seems to know things they

shouldn't, such as who you have been talking with, what you said and where you'll be.
    - Never remove spyware without a safety plan and lots of support because the abusive person will likely escalate their violent behaviour. It's also best to completely replace the device and immediately change all account passwords.
    - For more info, see: https://lukesplace.ca/resources/tech-abuse/spyware/

Under the "G"

- Privacy settings
    - If you have your privacy settings set the way you want, mark this spot.
    - Depending on what you want the world to see in your social media accounts, you may want to change your settings. Look for "Privacy" in the settings for your social media and other accounts.
    - You can check how your account appears publicly for most social media. Search for "how does my [Instagram/Facebook/Twitter/TikTok] appear publicly". Note that sometimes there are "hacks" for seeing some private accounts publicly (e.g. TikTok)
- Sexting
    - If you know what sexting is, mark this spot.
    - Sexting is the sharing of intimate images by a digital means, usually by messaging apps. Sexting is your choice. However, keep in mind that sometimes the person receiving your image may not treat your photo respectfully in the future.
    - Safer sexting tips:
        - Don't let someone push you into sharing.
        - Make sure the person you're sharing with is into receiving your intimate images.
        - Communicate what you are consenting to ("I'm really into sharing this with you, but don't let anyone else see it.")
        - Share only through a messaging service that doesn't have your name or contact info and that provides good security (e.g. Signal). Avoid sharing through WhatsApp which is a popular target for hackers looking for just this sort of thing.
        - Avoid including things that might identify you in the image, like your face, birthmarks, tattoos and surroundings.
        - Manage how your images are stored on your phone, in your messaging account and if there's a backup (e.g. on the cloud).
- Ask Google to remove a website from search results
    - If you knew you could do this, mark the spot
    - If someone has posted abusive information about you on the web, such an image you did not give them consent to share, you can ask Google to remove the page from their search results: https://support.google.com/legal/answer/3110420

- Phishing
    - If you know what phishing is, mark this spot.
    - Phishing is a malicious attempt to get sensitive information (like passwords or personal info), to gain access to your account or to get you to download malware.
    - Phishing is common with email. That's why spam filters were created. Sometimes these emails will still get through. Phishing also happens by text and through social media.
    - Often phishing will be disguised as a trusted source, like a contact or a well-known business or institution (e.g. UPS, Facebook, Canadian Revenue Agency, bank)
    - For information on how to identify phishing
        - In email: https://www.tessian.com/blog/what-does-a-spear-phishing-email-look-like/
        - In social media: https://www.trendmicro.com/en_us/what-is/phishing/social-media-phishing.html#facebook-phishing-tm-anchor
- Get consent before you share/post
    - If you ask people if you can share or post their photo, mark the square.
    - You may not know if someone is dealing with online harassment or a stalker or has other safety and privacy concerns. Perpetrators often monitor their victim's friend circles to learn more about the person and can gain access to images and other information that way.
    - If you know someone who's dealing with abuse, check your feed to see if you're sharing information that could endanger them. Ask your friends, family and workplace to do the same for you.

Under the "O"

- Blocking
    - If you know what blocking is, mark the spot.
    - If someone is harassing you in social media or through a messaging app, you may want to block them, which means you will not see their messages anymore. With some apps this means the person will very quickly learn you have blocked them, but in others it will take longer for them to figure it out. If you are dealing with an abusive person, you should likely make a safety plan before you block them as it may mean the person will escalate their abuse.
    - Depending on the app and the situation you are dealing with, there may be other strategies that will help you manage this unwanted communication. Most apps provide a variety of choices. Some will let the sender know you've blocked them while other won't. Some provide other options like "Muting" or "Hide alerts" or "Read receipts". To learn about the options, visit: https://www.consumerreports.org/digital-security/can-people-tell-when-blocked-texting-social-messaging-apps-a9942470743/

- Cautious opening attachments & links
    - If you are cautious about clicking links or opening attachments, mark the spot.
    - Malware and links to dangerous sites are often sent by text or email. The person sending this might be someone you know who wants to infect your device with a virus or spyware. Or, if it comes from a phishing account, this is a malicious person trying to get your data or other sensitive information.
    - Always be cautious opening attachments or clicking links unless you understand the full context.
- Limit info on dating sites
    - If this makes sense to you, mark the spot.
    - Be cautious sharing personal information on dating sites, not just with other people but with the platform itself. Creeps use dating sites to meet people they can trick, manipulate, or otherwise prey upon. Hackers also are interested in dating sites because they contain a lot of user data that can be easily sold.
    - Select sites that have good security for their data and provide privacy options and tips for their users. Use a username that doesn't disclose your full name. To find out if a dating site has been hacked in the past, search for the name of the site and the words "data breach".
- There's support for tech abuse
    - If you know that there's support out there for tech abuse, mark this spot.
    - You can get support from local sexual assault agencies and other community organizations. There are places online where you can read ways to manage online violence and even connect with supports, like Heart Mob (iHeartMob.org) (mostly for journalists).
    - If you are dealing with abuse in social media, you can also report the abuse to the company. To learn how, visit: https://iheartmob.org/resources/safety_guides
    - Because many forms of online violence are crimes, you can also report to police.
    - Remember to collect evidence of any abuse you experience.
- Browse privately
    - Do you know a way manage your internet history? If yes, mark this spot.
    - You can delete browsing history from your browser by finding the "history" area of your browser and selecting and deleting sites you visited.
    - The main web browsers also give you the option to browse privately. To learn how, search "private browsing" and the name of the program you use to look at the web (e.g. Chrome, Safari, Firefox, Explorer).
    - When you finish web browsing with a private window, close the browser to erase your history. This is good to do if you are using a public computer.
    - Browser tools will not protect you from spyware and will provide limited or no protection from trackers or fingerprinters, which are other ways your online activities get monitored by third-parties. For information about browsing really privately, visit the Electronic Frontier Foundation's Cover Your Tracks tool: https://coveryourtracks.eff.org/