Utilities and Digital Financial Abuse

We all need electricity, natural gas, or oil to heat our homes and run our devices. Yet, abusers are increasingly finding ways to misuse these utilities to extend their power and control over a survivor.

As utilities have moved billing and accounts online, abusers have also been able to change account settings, stop payments, and impersonate survivors.

They have also found ways to use smart technology and apps to control utilities remotely.

How Utility Accounts Are Misused by Abusers

- If your home has smart thermostats and an abuser has access to the control app, they can use the app to raise or lower the temperatures remotely, making the home unbearable to live in or spiking your bill.
- If an abuser has access to your online utility accounts, they can cancel utility services, withhold bill payments, or change account passwords to block your access.

How to Protect Your Smart Technology from Abuse

- Choose smart devices (a smart light bulb, smart TV, smart Bluetooth speakers, thermostats, and assistants) from reputable brands that offer better security and privacy terms and have a customer service support line.
- Set up a separate email address used only with and for smart technology devices. Use a hard-to-guess, strong password unique to each of them.
- Review and adjust privacy settings and choose which information your device can gather about you. Avoid granting access to data it does not need to perform its tasks.
- Keep the login details to yourself since they may give an abuser access to changing settings on the device.
- Install updates regularly by searching for and installing updates of devices and smart home systems to stay protected with the latest security fixes.
- Secure your Wi-Fi using a strong password and review the list of connected devices to ensure only trusted devices have access.

How to Protect Your Utility Accounts from Digital Financial Abuse

- Call the utility company to confirm that only you can access the account and make changes.
- Request notifications regarding suspicious activity, such as excessive heat during warm months.
- If the account is currently in the abuser's name, consider opening a new one.
- Set up an email address the abuser doesn't know for login and bill receipts.
- Choose a strong password and enable two-factor authentication if possible.
- Decide between automatic payments, online banking, or cheques for paying invoices.

To help you decide:

- For recurring payments, automatic payments are ideal for fixed, recurring bills and ensure no late fees are incurred. However, there are risks for overdrafts if you don't monitor your account balance, and if there is an error in an invoice, the payment may go through before you catch it.
- For one-time or variable payments, online banking provides flexibility and control. This may not be ideal for people who don't have a secure Internet connection and for those whose accounts are vulnerable to hacking.
- When dealing with traditional vendors, cheques are still helpful for businesses or individuals who don't accept digital payments. There may

be a cost incurred for cheques, and the slower processing time may be inconvenient for some.

Technology-Facilitated Gender-Based Violence (TFGBV) is part of a continuum of violence that can be both online and in-person. If you or someone you know is experiencing TFGBV, you are not alone. You can use sheltersafe.ca to find a shelter/transition house near you to discuss options and create a safety plan. You don't need to stay in a shelter to access free, confidential services and support. For more information about digital financial abuse, see our full Digital Financial Abuse Toolkit.

This project was funded by TD Bank Group, through its corporate citizenship platform, the TD Ready Commitment.