Disaster Tips: Cyber Attack

Helping you avoid the stay online

Types Of Failure

Power Outage: The electricity goes out. This affects fridges, lights, fans, and medical devices.

Internet/Wi-Fi Outage: The power is on, but your modem stops working. You lose access to video calls, streaming, and online support apps.

Cyber Attack/Scam: A scammer tries to steal your money or personal information via fake emails, texts, or phone calls.

Device Failure: Your phone, tablet, or laptop breaks or runs out of battery.

Be Prepared

Having a plan before something breaks is the key to staying calm.

The "Offline" Contact List: Write down the phone numbers of your key support people (Support Coordinator, family, Support Workers) on paper.

Backup Power Plan: Buy a power bank (portable phone charger) and keep it fully charged.

Auto-Save: Turn on "auto-save" for your documents so you don't lose work if the computer crashes

During a Power or Internet Outage

Use Mobile Data: If your home Wi-Fi is down, turn on the "Hotspot" on your mobile phone.

Manual Check-ins: If you usually have a support worker, call you via video, agree on a backup plan.

Keep the Fridge Closed: During a power outage, keep fridge and freezer doors shut. Food stays cold for up to 4 hours in the fridge and 24 hours in a half-full freezer.

Stay Warm/Cool: If the power goes out in summer, use our heatwave tips. If it's winter, layer up with blankets.

Cyber Safety

Scammers often target people who are isolated or less familiar with technology.

The "Slow Down" Rule: If someone calls, emails, or texts you asking for money, passwords, or gift cards – stop. Take a breath. A real company will never rush you.

Do Not Click Links: If you get a text or email claiming to be from a service you us – do not click on any links. Open a new browser window and go directly to the official website instead.

If in Doubt, Hang Up: If a caller says they are from the "NDIS" or "Bank" and asks for your password, hang up immediately. Call the official number for the NDIS or your bank and let them know someone might be trying to access your account.

If Your Device is Hacked or Infected

Disconnect: Turn off your Wi-Fi and unplug your modem to stop the hacker from accessing your files.

Run a Scan: If you have antivirus software (like Norton or McAfee), run a full system scan.

Change Passwords: Using a different device (like a friend's phone), change your most important passwords (banking, email, NDIS).

Report It: Report cyber scams to ReportCyber (1300 292 371). If money was stolen, call your bank immediately.

Repair: Take your device to an IT specialist and ask them to recover your device, this might entail reinstalling your operating system so be sure to ask that your files be backed up.

Things to Avoid

DO NOT use the same password for everything. If one site gets hacked, they will try that password on your bank and email.

DO NOT post your travel plans or daily routines publicly on social media (like Facebook or TikTok) – strangers can use this to target your home.

DO NOT open email attachments from people you don't know.

DO NOT wait until your battery is at 1% to charge it. Charge your devices whenever you have power.

DO NOT forget to update your software. Those "update" pop-ups often fix security holes, so click "Update" when you can (just make sure it's a real notification from your device settings).

Staying Informed

Network Outages: Check the website "DownDetector" (if you have mobile data) to see if your internet provider is down nationally.

Power Outages: Call your electricity provider's fault line or check their app.

Local Radio: Keep a battery-powered radio. Local ABC radio stations give updates on major power outages in your area.