



Cyberattacks, GPS and grid failures

Cyberattacks, IT failures and severe space weather can knock out power, payments, navigation and online services, and scammers often exploit the confusion. This page helps your family secure accounts, keep offline backups, and avoid outage scams.

CHECKLIST

- | | |
|---|--|
| ☐ Cash in mixed small denominations | ☐ External hard drive with backups of key files |
| ☐ Bank cards from more than one provider, PINs memorised | ☐ Solar or hand-crank phone charger |
| ☐ Printed local maps | ☐ Car phone charger |
| ☐ Paper list of important phone numbers | ☐ Battery or wind-up radio |

BEFORE

- Protect your email first with a strong unique password or passkey and 2-step verification.
- Use a password manager to create and store different passwords for each account.
- Switch on automatic updates for phones, computers and smart home devices.
- Back up photos and key documents, ideally automatically or at least weekly, and practise restoring them.
- Keep some cash at home in mixed small notes, and hold cards from more than one provider.
- Keep printed maps and a paper contact list in case GPS and phones stop working.

DURING

- In a severe space weather alert, save electricity to help prevent forced power cuts.
- Keep phone calls for emergencies only, and avoid lifts in case power fails.
- Follow official emergency alerts and instructions carefully.
- Treat unexpected messages about the outage with suspicion, even if they look official.
- Watch for scam signs: urgency, threats, claims of authority, or offers that play on fear.
- Do not click links, scan QR codes or download fixes from unsolicited messages.
- Check any request by contacting the organisation through its official website, not the message.
- Remember banks never ask you to confirm account details by email or phone.

AFTER

- Report scam messages and websites so authorities can take them down.
- If you think you were scammed, report it to the police straight away.
- Report suspected fraud quickly, even if you feel embarrassed. Fast reports help.
- Restore any lost or damaged files from your backups.

IN THE UAE

In the UAE, report online scams and cyber-enabled fraud through the Dubai Police eCrime platform (ecrimehub.gov.ae) or your local police. For emergencies, call police on 999.

MY NOTES

Sources: UK Government (Prepare), Cyber (<https://prepare.campaign.gov.uk/be-informed-about-hazards/cyber/>); UK National Cyber Security Centre (NCSC), Top tips for staying secure online (<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online>); US National Weather Service (NOAA), Before an Extreme Solar Event (<https://www.weather.gov/safety/space-before>); Swedish Civil Contingencies Agency (MCF), Payments and cash in times of crisis (<https://www.mcf.se/en/advice-for-individuals/home-preparedness--prepping-for-at-least-a-week/payments-and-cash-in-times-of-crisis/>); UK Government (Prepare), Phone and broadband outages (<https://prepare.campaign.gov.uk/be-informed-about-hazards/phone-broadband-outages/>); US National Weather Service (NOAA), During an Extreme Solar Event (<https://www.weather.gov/safety/space-during>); UK National Cyber Security Centre (NCSC), Statement on major IT outage and phishing threat (<https://www.ncsc.gov.uk/news/major-it-outage>); UK National Cyber Security Centre (NCSC), Spot scams (<https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams>); UK National Cyber Security Centre (NCSC), Phishing attacks: defending your organisation (<https://www.ncsc.gov.uk/guidance/phishing>); UAE Government Portal ([u.ae](https://u.ae/en/information-and-services/business/important-digital-services/reporting-economic-crimes)), Reporting economic crimes (<https://u.ae/en/information-and-services/business/important-digital-services/reporting-economic-crimes>)

General guidance in our own words. Always follow your local authorities.