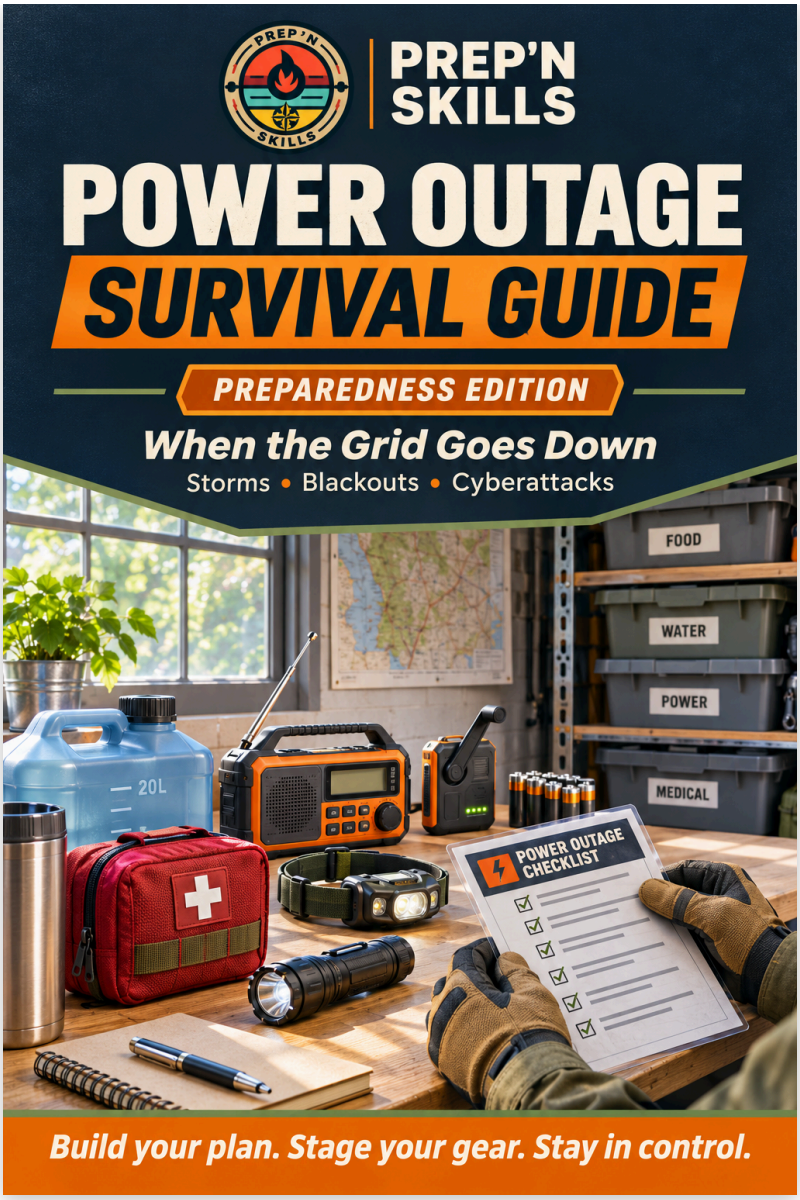


The Power Outage Survival Guide

When the grid, the network or the cloud goes down: what governments now tell households to have, what actually fails at home, and the 72-hour plan.

Free from Prep'N Skills · prepnskills.com

© 2026 Prep'N Skills. All rights reserved. You're welcome to share this PDF whole and unchanged; please don't sell it or pass parts of it off as your own.

This guide is general preparedness information for educational purposes. It isn't medical, legal or professional advice, and it doesn't replace instructions from local officials, your utility, your doctor or a device's manufacturer. In an emergency, call **911**.

Every number in this guide comes from a government agency, a regulator, a company's own incident report or a major news wire, and each chapter lists its sources. Where an official source gives no number, the guide says so instead of guessing. Facts were checked in November 2026.

How to Use This Guide

Read Chapters 1 and 2 first. They explain why so many governments now ask households to be ready for 72 hours or more, and what has actually gone down in the last few years. Most of it wasn't an attack.

Then read the chapter that worries you most:

If you're worried about	Read
Attacks on the power grid, water or food supply	Chapter 3
Scam calls, fake disaster charities and AI voice clones	Chapter 4
What stops working at home: cards, phones, 911, pharmacies, gas	Chapter 5
Getting into your accounts and paying for things offline	Chapter 6
What to do, day by day, for the first 72 hours	Chapter 7

Every chapter ends with "Do this now": three to six things you can do this week. Do those and you're ahead of most households.

Contents

- Chapter 1 · Why Governments Now Say 72 Hours, or a Week
- Chapter 2 · The Outage Record
- Chapter 3 · How AI Changes the Attacks on Power, Water and Food
- Chapter 4 · How AI Changes the Scams That Follow a Crisis
- Chapter 5 · What Fails at Home When the Systems Go Down
- Chapter 6 · The Offline Backup Kit
- Chapter 7 · Crisis Cyber Hygiene and Your 72-Hour Plan
- Your Next Step

Chapter 1: Why Governments Now Say 72 Hours, or a Week



Between April 2024 and November 2026, **11 countries and the European Union** issued **17** new pieces of guidance telling households to keep their own supplies at home. Every one of them set a number: **3 days** at the least, a **week** in Norway, Sweden and Estonia, and **10 days** as the ideal in Germany. The United States is the exception. Its guidance asks for "several days" and names no number at all.

That gap is the reason this guide exists. The rest of the democratic world has told its citizens how long to plan for. Americans have to pick the number themselves.

The wave, in order

Several governments mailed the advice straight to people's homes.

When	Who	What households are told
Spring 2024	**Estonia**	At least **7 days**; instructions mailed to more than **566,000** homes

June 2024	**Denmark**	**3 days**, relaunched as a national campaign in November 2025
Spring and autumn 2024	**Norway**	**One week**, with a new brochure sent to every household
November 2024	**Sweden**	At least **one week**; more than **5 million** copies of *If Crisis or War Comes* mailed
November 2024	**Finland**	**72 hours**
March 2025	**European Union**	A minimum of **72 hours**, set as the target for member states
2025	**Poland**	At least **3 days**
2025	**Germany**	Ideally **10 days**, at least 3
November 2025	**Netherlands**	**72 hours**; a booklet to more than **8.5 million** households
October 2026	**United Kingdom**	**3 days**, the start of a three-year "Be Ready" campaign
November 2026	**Japan**	At least **3 days**, ideally **a week**

Three days is the floor everywhere on that list. No government asks for less.

What they say they're preparing for

The booklets explain themselves, and the explanations have changed. Storms and floods are still there, but they now share the page with war, sabotage and attacks on computer systems.

- **Norway's** brochure says people live in "an increasingly turbulent world, partly as a result of climate change, war and digital threats." It warns that a power cut can stop tap water, sewerage, **payment systems, the internet and mobile phones**.
- **Denmark's** 2024 launch says the threat from "cyberattacks and sabotage has increased as a result of the worsened security situation in Europe." Its 2025 campaign calls the present "the most serious risk and threat picture since the Second World War."
- **Poland's** 2025 guide names "disinformation, cyberattacks, hybrid threats, sabotage" and the war across its eastern border. It has a whole section on a long **blackout**.
- **The Netherlands** says "geopolitical developments and climate change" make an emergency more likely, and that "most people are on their own for the first **72 hours**."
- **Estonia** gives the plainest reason of all: "The bigger the crisis, the longer it takes for local-government or state help to reach you."

That sentence is the logic behind the numbers. Norway spells out the rest: municipalities and emergency services "must prioritize those who can't manage without help in a crisis." A household that can manage alone for three days, or seven, leaves responders free for the people who can't.

Where the United States stands

Ready.gov, FEMA's preparedness site, tells Americans: "After an emergency, you may need to survive on your own for **several days**." It asks for water at **1 gallon per person per day** and "at least a several-day supply" of food. It gives no number of days. Older federal material said "at least three days"; the current pages don't.

At the same time, Washington has been moving the job of preparing toward households:

- A **March 2025** executive order says preparedness "is most effectively owned and managed at the State, local, and even individual levels."
- The **FEMA Review Council's** final report, approved in **May 2026**, calls on "every American to embrace their individual responsibility" by being prepared for disasters. It sets no number of days either.

So the guidance in the U.S. has become vaguer about how much to store while saying more clearly that storing it is your job.

The number this guide uses

This guide sets **72 hours as the floor and one week as the goal.** That's the guide's own choice, not a U.S. government standard, and it matches what most of the countries in the table ask for.

Here's what the floor and the goal mean for water, at Ready.gov's rate of 1 gallon per person per day:

People	72 hours	One week
1	**3 gallons**	**7 gallons**
2	**6 gallons**	**14 gallons**
3	**9 gallons**	**21 gallons**
4	**12 gallons**	**28 gallons**
5	**15 gallons**	**35 gallons**

Worked out as people × 1 gallon × days. Ready.gov notes water needs can double in very hot weather.

Start with the 72-hour column. A household of four needs **12 gallons**: four 24-packs of 16.9-ounce bottles hold just over that (each case is **3.17 gallons**). Build toward the week once the floor is in place.

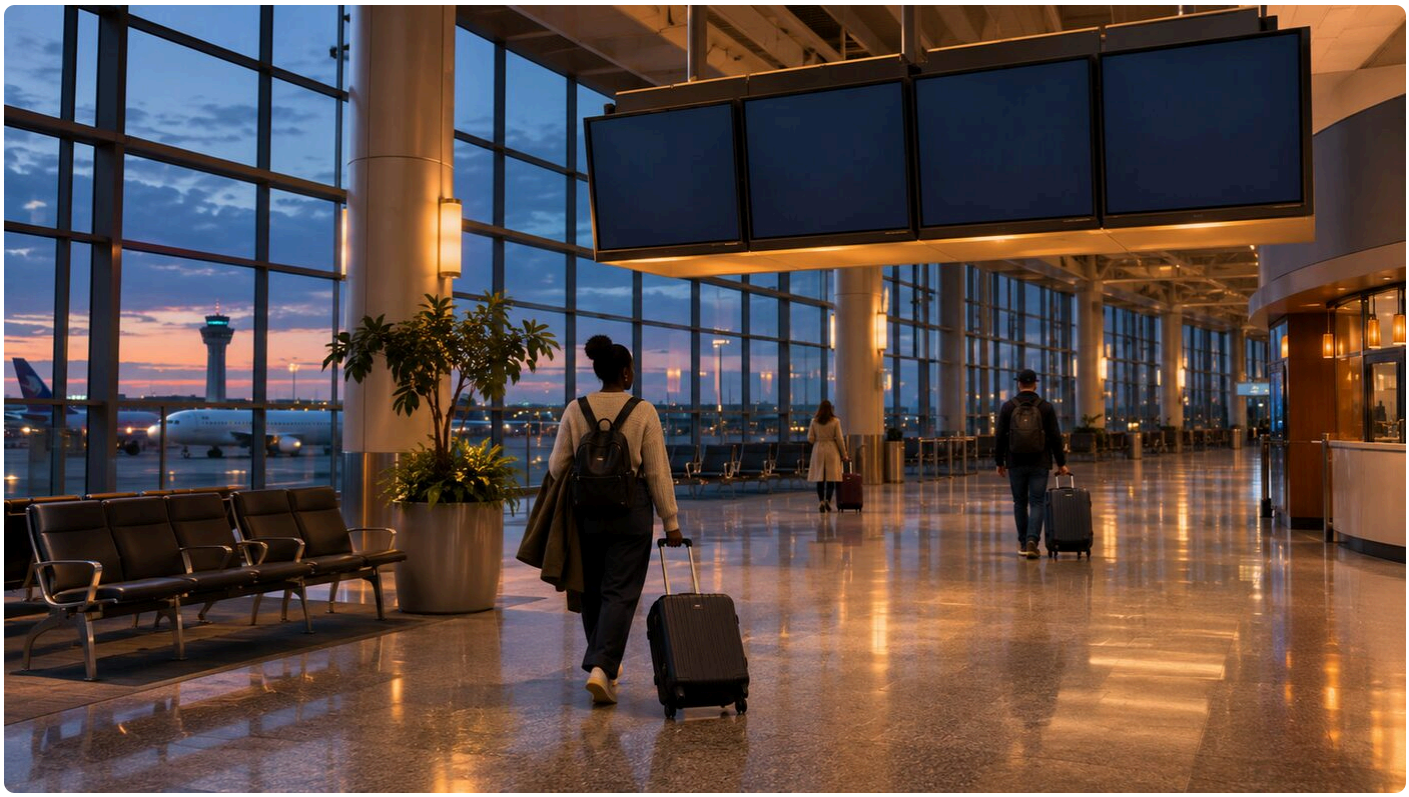
Why it matters now

Several of these booklets plan for a long power cut, a broken payment system or a phone network that can't connect, not only for a storm. The next chapter shows those failures aren't hypothetical. Most of them have already happened in the United States, and most of them had nothing to do with an attack.

Do this now

- [ ] Count the people in your household and write down your **72-hour water number** (people × 3 gallons)
- [ ] Write down your **one-week number** (people × 7 gallons) as the next goal
- [ ] Check what you already have: water, food that needs no cooking, a flashlight per person
- [ ] Decide where the supplies go before you buy them

Chapter 2: The Outage Record



Of the **nine** major outages on this guide's shortlist, from 2021 to 2026, only **two** were attacks. The other seven came from bad updates, configuration mistakes, software defects, deleted files or a grid that failed on its own, and each still cut ordinary people off from something they use every day.

A household plan built only for hackers misses most of the record. The system fails whether anyone attacks it or not, and the plan is the same either way.

Nine outages, two attacks

The table gives each cause as officially stated.

When	What failed	Cause, as officially stated	Attack?
May 2021	**Colonial Pipeline**	Ransomware by the criminal group **DarkSide** (Colonial CEO)	**Yes**
Jan 2023	**FAA NOTAM** flight-safety system	Contract staff "unintentionally deleted files"; "no evidence of a cyber-attack" (FAA)	No
Feb 2024	**Change Healthcare** claims and pharmacy network	A cyberattack (HHS; UnitedHealth Group)	**Yes**

Feb 2024	**AT&T** wireless, nationwide	"An equipment configuration error" (FCC)	No
Jul 2024	**CrowdStrike** update on Windows computers	"Not the result of or related to a cyberattack" (CrowdStrike)	No
Apr 2025	**Spain and Portugal** power grid	Spain's energy minister ruled out a cyberattack (Euronews)	No
Oct 2025	**Amazon Web Services**, main U.S. region	"A latent defect" in its own DNS automation (AWS)	No
Jan 2026	**Verizon** wireless	"A software issue"; "no indication that this was a cybersecurity issue" (Verizon)	No
Nov 2026	**Microsoft 365**, Outlook and Teams	A "technical issue", not a cybersecurity breach (Microsoft, via CNN)	No

Seven of nine is a count of this table, not a national statistic.

The seven failures

By each official account, seven outages on the shortlist were not attacks.

AT&T, 22 February 2024. An AT&T network change with "an equipment configuration error" went in at **2:42 a.m.**, and the nationwide outage began three minutes later. The FCC found it lasted "at least twelve hours", hit "more than **125 million** registered devices", blocked "more than **92 million** voice calls" and stopped "more than **25,000** calls" to 911 centers. Users were affected in all **50** states, Washington, D.C., Puerto Rico and the U.S. Virgin Islands. Phones showed "SOS", and even SOS-mode 911 calls over AT&T failed. Wi-Fi calling, the workaround AT&T suggested, returned a "502 Bad Gateway" error for some users.

Verizon, 14 January 2026. The FCC says Verizon "suffered a service outage that lasted at least ten hours and affected millions of customers", many of whom could not make or receive calls and texts. Verizon called it "a software issue". The FCC has published no findings yet. Its notice cites a customer who had to borrow another carrier's phone to reach 911.

CrowdStrike, 19 July 2024. A faulty update to CrowdStrike's Falcon security software triggered "a logic error resulting in a system crash and blue screen" on Windows machines. Microsoft estimated it hit **8.5 million** Windows devices. The bad file was live for **78 minutes**, worked out from CrowdStrike's own times of 04:09 to 05:27 UTC, but machines that had already crashed needed hands-on repair, so recovery took days. Flights, hospitals and banks were disrupted. Microsoft said it "was not a Microsoft incident".

FAA, 11 January 2023. The Notice to Air Missions system, which gives flight crews safety information, failed overnight, and the FAA ordered airlines to "pause all domestic departures until 9 a.m. Eastern

Time". Its preliminary review found contract staff "unintentionally deleted files" while fixing synchronization between the live database and a backup. FlightAware counts reported by the press put delays at more than **9,500** U.S. flights and cancellations at about **1,300** by that afternoon.

Spain and Portugal, 28 April 2025. At **12:33 CEST**, ENTSO-E reports, "the power systems of continental Spain and Portugal experienced a total blackout." Euronews reported "tens of millions disconnected in seconds", Spain's loss of **15 gigawatts**, "equivalent to **60%** of its supply", and power back by the early hours of the next day. It also reported that Spain's energy minister "explicitly ruled out a cyberattack", with the government's report blaming "technical and planning errors".

Amazon Web Services, 19 to 20 October 2025. AWS says the event "was triggered by a latent defect within the service's automated DNS management system". It ran from 11:48 p.m. to 2:20 p.m. Pacific, which works out to **14 hours 32 minutes** from AWS's own start and end times. News reports listed Venmo, Snapchat, Ring doorbells, Coinbase, Robinhood and some banks among the services that went down.

Microsoft 365, 12 to 13 November 2026. Outlook and Teams went down worldwide, starting midday on the U.S. East Coast. Microsoft said it was not a cybersecurity breach and blamed "an issue during an earlier network capacity upgrade". CNN reported that schools asked parents to phone in absences and some local governments told residents to call instead of email. Microsoft has not published a final review, so the details are provisional.

The two that were attacks

Both attacks were criminal ransomware.

Colonial Pipeline, 7 May 2021. Colonial's CEO told the Senate the company was hit by "a ransomware attack by the cyber-criminal group DarkSide." The ransomware hit Colonial's IT network, and the company shut the pipeline as a precaution "to help ensure that the malware was not able to spread" to the systems that run it. By 6:10 a.m. "all **5,500 miles** of pipelines had been shut down." That pipeline carries "nearly half of the fuel consumed on the East Coast", serving "more than **50 million** Americans". It began returning to service on the evening of 12 May, about **5 days** later. CISA describes "snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel."

Change Healthcare, February 2024. HHS said a "cybersecurity incident in late February" left hospitals, doctors and pharmacies with cash-flow problems "stemming from an inability to submit claims and receive payments." Pharmacies could not process insurance claims or e-prescriptions for weeks. UnitedHealth Group, which owns Change Healthcare, said on 22 April that pharmacy services were "back to near-normal levels, with **99%** of pre-incident pharmacies able to process claims." UnitedHealth later estimated that data on about **190 million** people was exposed, as reported by Fierce Healthcare. It was a billing and pharmacy shutdown, not a power cut.

What the pattern means for a household

The cause matters to investigators, not at the kitchen table. The AT&T customer who couldn't reach 911 and the East Coast driver in a gas line faced the same problem: a service that was there one morning and gone the next. Two points come straight out of the record:

- **The fallbacks fail too.** AT&T's own workaround, Wi-Fi calling, broke for some users. A backup that runs on the same network as the main service isn't a backup.
- **Recovery outlasts the fault.** CrowdStrike's bad file was live for **78 minutes**; repairs took days. Change Healthcare's attack surfaced in late February; UnitedHealth reported pharmacies near-normal on 22 April.

The next chapter covers the attacks that are aimed at power and water, and what AI changes about them. Chapter 5 walks through each link in the household chain these outages broke: cards, phones, prescriptions, fuel, water, food and the cloud.

Do this now

- [ ] List the services your household uses from the table: your cell carrier, your pharmacy's insurance billing, your work computer, your email, your fuel supply
- [ ] Pick a second way to reach 911 that doesn't run through your main phone network: a landline, a phone on another carrier, or satellite SOS (this guide's suggestion, drawn from the AT&T report)
- [ ] Ask your pharmacist about "maintaining an emergency supply" of daily medicines, as the FDA advises
- [ ] Keep a small amount of cash in small bills at home, which Ready.gov advises "because ATMs and credit cards may not work during a disaster"

Chapter 3: How AI Changes the Attacks on Power, Water and Food



AI lowers the barrier for attackers and speeds up their attacks, according to the cyber agencies of the Five Eyes countries, and a U.S. advisory from **August 2026** says attackers already use it against controllers in energy, water and food plants. The weaknesses named on the official record are old ones, such as default passwords, and this guide's research found **no confirmed 2026 U.S. power outage** caused by a cyberattack of any kind.

The threat is official. The household plan for it is the same plan that covers any other outage.

What the agencies say AI changes

In **June 2026** the heads of six cyber agencies, from the **United States, the United Kingdom, Canada, Australia and New Zealand**, signed a joint statement titled *The AI shift in cyber risk: why leaders must act now*. Two lines from it:

- "AI is not a future consideration – it is already here."
- "It lowers barriers for malicious actors and increases the speed and complexity of attacks."

On **August 19, 2026**, the **NSA, CISA, FBI, Department of Energy and EPA** issued advisory **AA26-231A** on **Siemens S7** programmable logic controllers (PLCs), the controllers that run equipment in

energy, water and food plants. It says: "Threat actors are using AI assistance to generate exploitation scripts." It calls this "an active threat," not "a theoretical risk."

Its most-targeted sectors include **Energy**, **Water and Wastewater**, and **Food and Agriculture**. It names no country behind the activity.

The record: which attacks involved AI

One entry in the official record behind this chapter carries an AI link. The table gives each cause as the authorities stated it.

When	Target	What happened	Who, per officials	AI link in the sources
December 2015	Ukraine's grid	**3** power companies hit within **30 minutes**; **225,000** customers lost power for **1 to 6 hours**	Russian state-sponsored actors (CISA)	None
December 2016	Kyiv's grid	Part of the capital lost power; restored in about **1 hour 15 minutes**	Russian state-sponsored actors (CISA)	None
November 2023	A U.S. water facility	A **Unitronics** controller "likely accessed"; the water authority "switched to manual operations"	Not named in the CISA alert	None
February 2024	U.S. energy, water, communications, transport	**Volt Typhoon** found inside IT networks	PRC state-sponsored (CISA, NSA, FBI)	None
July 2026	U.S. water and wastewater	Activity targeting "more than **100**" entities	No official attribution	None
August 2026	Siemens S7 controllers	Advisory AA26-231A: AI-assisted exploit scripts in active use	No country named	**Yes**
October 2026	About **700** French supermarkets	Fridges pushed to **50°C (122°F)**	Iran's IRGC (French government)	None

November 2, 2026	Stores in several more European countries	Freezers hit the same way	No official attribution	None

Worked out from the table: **1 of the 8** entries carries an AI link in the official sources; the other 7 carry none.

The DOE and DHS called the 2015 Ukraine attack "the first known cyber-enabled disruption of electricity service." The 2016 restoration time comes from Ukraine's grid operator by way of news reports, not from a U.S. agency.

On Volt Typhoon, CISA, the NSA and the FBI said in **February 2024** that PRC state-sponsored actors "are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks" against U.S. critical infrastructure "in the event of a major crisis or conflict with the United States." The advisory says Volt Typhoon has compromised IT environments of organizations in energy and water, among other sectors.

Water systems: what EPA inspectors found

Over 70% of the drinking water systems EPA inspected from **September 2023** were in violation of basic requirements of the Safe Drinking Water Act, EPA said in **May 2024**. The gaps were ordinary ones. EPA found that "some water systems failed to change default passwords, use single logins for all staff, or failed to curtail access by former employees."

EPA spelled out what an attacker could do with that access: "disrupting the treatment, distribution, and storage of water for the community, damaging pumps and valves, and altering the levels of chemicals to hazardous amounts." It also warned that attackers "may have embedded the capability to disable them in the future."

The **November 2023** case shows the same weakness. CISA said the attackers "likely accessed" the controller "by exploiting cybersecurity weaknesses, including poor password security and exposure to the internet." Its advice to utilities: make sure the default password **"1111"** is not in use. CISA reported "no known risk to the municipality's drinking water or water supply."

In **July 2026**, CISA observed activity targeting **more than 100** water and wastewater entities. CISA's word is "targeting," not "compromised," and its page names no actor. This guide's research found no official report of unsafe tap water from it, and no official source linking it to AI.

Food: the supermarket refrigeration hacks

On the night of **October 11 to 12, 2026**, attackers pushed refrigerators at about **700** of France's **10,000** supermarkets to **50°C (122°F)** for about six hours, AP reported. Stores threw out fresh and frozen food. The Paris prosecutor reported significant food losses and about twenty fires. Intermarché reported losses of "tens of millions of euros" in a single day.

France blames Iran. Foreign Minister Barrot said the attack "was carried out by the Islamic Revolutionary Guard Corps (IRGC)," and France's national cybersecurity agency, ANSSI, attributed it to

an IRGC-affiliated unit. Iran calls the accusation "baseless and biased." No individual has been charged.

On **November 2, 2026**, supermarket freezers in several more European countries, **Sweden** and **Belgium** among them, were hit the same way. One Swedish store reported freezers set to 50°C (122°F); a Swedish grocer's home-delivery warehouse was also hit. No government has named who did it. The joint statement from ENISA, the European Commission and Europol says member states are "currently investigating." Claims posted by hacker groups are claims, not attribution.

Neither wave is described as AI-enabled in the official sources. This guide's research found no U.S. supermarket refrigeration hack.

What AI does not change

The weak points on the record are older than the AI warnings: default passwords, shared logins, former staff who kept access, and controllers left open to the internet. The CISA, EPA and FBI fact sheet for water utilities (**February 2024**) lists "Reduce Exposure to the Public-Facing Internet" first and "Change Default Passwords Immediately" third.

AI does not change the household plan either. A tap that stops because of a fault and a tap that stops because of a hack leave the same empty glass. Ready.gov says a regular water source "could be cut-off or compromised through contamination," and asks for **1 gallon per person per day**. CDC asks for that gallon "for 3 days" and says to "Try to store a 2-week supply if possible." Chapter 1 turns that rate into a number for each household size.

The same holds for food. At home, a refrigerator keeps food safe "for up to 4 hours" without power, and a full freezer holds about **48 hours** (**24 hours** half full), according to FoodSafety.gov. Chapter 5 follows each of these failures into the house, link by link. Chapter 4 covers the other place AI shows up: the scams that follow a crisis.

Do this now

- [ ] Store water at **1 gallon per person per day**, starting with the 72-hour number from Chapter 1
- [ ] Mark the date on stored water and replace it every **6 months**, as CDC advises for filled containers
- [ ] Put a thermometer in the refrigerator and freezer; Ready.gov says to throw out food at **40 degrees** or higher
- [ ] Write your water utility's phone number on paper, with your other emergency numbers

Chapter 4: How AI Changes the Scams That Follow a Crisis



In 2025 the FBI's Internet Crime Complaint Center (IC3) logged **22,364** complaints involving AI and **$893,346,472** in losses, the first year it published an AI category at all. People **60 and over** filed a small share of those complaints but carried close to **40%** of the money lost.

The same tools fake a familiar voice on the phone and a photo of a disaster. The defenses the FBI and FTC recommend cost nothing, a call back and a family code word, but they have to be set up before the crisis, not during it.

What the FBI counted in 2025

The FBI's **2025 Internet Crime Report** splits the AI figures by age:

AI-related complaints, 2025	Complaints	Losses
Everyone	**22,364**	**$893,346,472**
Age 60 and over	**3,143**	**$352,496,231**
60+ share	**14.1%**	**39.5%**

60+ share worked out as 3,143 / 22,364 = 14.1% and $352,496,231 / $893,346,472 = 39.5%, from the IC3 2025 report's AI section and its 60+ tables.

The average AI complaint from someone 60 or older carried about **$112,000** in losses, against about **$28,000** for the rest of the AI complaints, roughly four times as much. *Worked out as $352,496,231 / 3,143 = $112,153, and ($893,346,472 – $352,496,231) / (22,364 – 3,143) = $28,139. The "rest" includes complaints with no age given.*

The report also breaks out two schemes:

- **Voice-clone "distress" scams:** victims claimed losses **over $5 million** in 2025. IC3 describes these as grandparent scams "in which voice cloning technology is used to mimic the sound of a loved one in distress."
- **Investment scams with an AI link: more than $632 million**. IC3 adds that overall investment losses passed **$8 billion**, which it says shows "many victims do not realize the extent AI may be involved in scams."

The **$5 million** voice-clone figure is the only official loss number specific to voice cloning this guide found. The Federal Trade Commission counted **over $3.5 billion** lost to impostor scams in 2025 but publishes no separate figure for AI or voice cloning.

The voice on the phone is not proof

The FBI says criminals "generate short audio clips containing a loved one's voice to impersonate a close relative in a crisis situation, asking for immediate financial assistance or demanding a ransom." A **May 2025** FBI warning goes further: a cloned voice and the real one "can sound nearly identical," and "AI-generated content has advanced to the point that it is often difficult to identify."

So listening harder is no defense. The agencies give three checks that don't depend on your ear:

1. **The FTC:** "Don't trust the voice." Its 2023 alert on AI family-emergency scams says to "call the person who supposedly contacted you and verify the story."
2. **The FBI:** hang up, look up the real number of the bank or organization that claims to be calling, and "call the phone number directly."
3. **The FBI again, in December 2024, repeated in May 2025:** "Create a secret word or phrase with your family to verify their identity."

The family code word is the one check that still works when the call-back fails. Chapter 5 covers what happens to phones and 911 in an outage. When the real relative can't be reached, ask the caller for the word.

The FBI's list of what to refuse holds in any emergency: "Do not send money, gift cards, cryptocurrency, or other assets to people you do not know or have met only online or over the phone." The FTC's voice-clone alert names the same red flags: a caller who asks you to wire money, send cryptocurrency or buy gift cards.

What the law says about AI voices in robocalls

On **February 2, 2024**, the Federal Communications Commission ruled that AI voices count as "artificial" under the Telephone Consumer Protection Act. In the FCC's words, voice cloning falls under the law "because this technology artificially simulates a human voice," and callers "must obtain prior express consent from the called party" before using it. A robocall in a cloned voice, made without that consent, breaks federal law.

The ruling adds that voice cloning "can convince a called party that a trusted person, or someone they care about such as a family member, wants or needs them to take some action that they would not otherwise take." The ruling sets the law; it doesn't screen the call, so the code word and the call-back remain the household's defense.

Fake aid after a disaster

After a disaster, scammers impersonate FEMA itself. FEMA's own fraud warnings come down to one rule: **FEMA does not charge for disaster aid.**

What the agencies say	Source
"FEMA doesn't charge people for disaster assistance."	FTC, July 2025
"FEMA never charges a fee for an inspection."	FEMA, Disaster Fraud page
"All FEMA employees carry a photo ID badge."	FEMA, December 2025
"Don't give banking information to a person claiming to be a FEMA inspector."	FEMA, December 2025
"Never trust anyone asking for money in exchange for disaster aid or promising grants in return for large deposits."	FEMA, April 2026

The FTC put it plainly after Hurricane Helene in **October 2024**: "If someone asks you for money to help you qualify for FEMA funds, it's a scam."

AI makes the fake official more convincing. A **September 2026** FBI warning reports that IC3 received **nearly 61,000** complaints of law-enforcement or government impersonation between January 2025 and July 2026, with losses **over $1.6 billion**. The FBI says AI and other new technologies "allow scammers to appear as law enforcement and government officials on video calls with victims." An official's face on a video call proves nothing on its own.

To check whether a FEMA contact is real, call FEMA directly at **1-800-621-3362**. To report a suspected fraud, call the National Center for Disaster Fraud at **1-866-720-5721**.

Fake pictures, fake charities

The FBI warned in **December 2024** that "criminals use generative AI tools to create images of natural disaster or global conflict to elicit donations to fraudulent charities."

A **January 2025** report from the Department of Homeland Security's Science and Technology Directorate says that during the **2023 Maui wildfires**, a Chinese influence operation used social media "to amplify AI-generated fabricated images of the wildfires." The same report warns that "emergency and disaster management missions are increasingly threatened by AI-synthesized fake media."

FEMA's rumor pages, the general one updated in **June 2026** and the Helene and Milton page that is still live, say nothing about AI-made images. No FTC or CISA disaster-scam alert this guide found mentions them either. The FTC, the Justice Department and the CFPB did warn in **October 2024** about "fraudulent charities soliciting donations for disaster victims," without mentioning AI.

The FBI lists what to look for in a fake image or video: "distorted hands or feet, unrealistic teeth or eyes," "inaccurate shadows, watermarks, lag time, voice matching, and unrealistic movements." AI content is now "often difficult to identify," so the safer test is the source, not the picture. CISA's advice after a disaster: "Before responding, ensure guidance is from trusted sources." FEMA asks the same: find trusted sources and share only from them.

Do this now

- [ ] Choose a **family code word** in person, and make sure every adult and older child knows it
- [ ] Post the rule where the whole household sees it: **hang up, then call back** on a number you already have
- [ ] Save FEMA's number, **1-800-621-3362**, and the disaster-fraud line, **1-866-720-5721**, on paper
- [ ] Refuse any payment by **wire, gift card or cryptocurrency** to someone who contacted you first
- [ ] Give to disaster relief only through a charity you look up yourself, never through a link in a post or message

Chapter 5: What Fails at Home When the Systems Go Down



Seven everyday systems sit between a household and its basic needs: cards, phones, prescriptions, fuel, tap water, grocery refrigeration and the cloud. Every one of them has failed in a verified real event since **2021**, and the official U.S. advice for each is short.

Worked out from the cases below: **4** links failed under attack and **3** failed through a software fault or a configuration error, with no attacker. The household plan is the same.

Link	Real failure	Cause	Official advice
Cards and ATMs	CrowdStrike, July 2024	Faulty update	Small bills at home
Phones and 911	AT&T, February 2024	Configuration error	Text first, keep a corded phone
Prescriptions	Change Healthcare, February 2024	Ransomware	Early refills, a copy of prescriptions
Fuel	Colonial Pipeline, May 2021	Ransomware	Half a tank at all times

Water	U.S. water facility, November 2023	Attack on a controller	Stored water
Grocery refrigeration	French supermarkets, October 2026	Attack on refrigeration	The 4-hour and 48-hour rules
Apps and the cloud	AWS, October 2025	Software defect	Backups and copies

Chapter 2 tells each outage in full.

Cards and ATMs

Card payments and cash machines stop when their computers stop. On **19 July 2024** a faulty CrowdStrike security update crashed an estimated **8.5 million** Windows devices, and banks were among the services disrupted. CrowdStrike said it was "not the result of or related to a cyberattack." A plain power cut does the same: Ready.gov says an outage may "Close retail businesses, grocery stores, gas stations, ATMs, banks and other services."

The official advice is cash. Ready.gov: "It is important to have small bills on hand because ATMs and credit cards may not work during a disaster." The **FDIC** said the same in August 2025. Neither names a dollar amount, and this guide found no official U.S. count of how often card networks fail during an outage. Chapter 6 covers the cash itself.

Phones and 911

A phone network can fail nationwide and take 911 with it. On **22 February 2024** an equipment configuration error knocked out AT&T's wireless network for **at least twelve hours**, blocking more than **92 million** calls and more than **25,000** calls to 911, according to the **FCC**. It was not a cyberattack. AT&T's recommended workaround, Wi-Fi calling, returned a "502 Bad Gateway" error for some users.

The FCC's advice:

- **Text first.** "In many cases text messages will go through when your call may not."
- **Keep a landline that needs no power.** "Be sure that you have at least one corded telephone that is not dependent on electricity."
- **Pause before redialing.** "Wait 10 seconds before redialing a call."
- **Call 911 by voice when you can.** "Text-to-911 is only currently available in certain locations."

The AT&T failure points to one more step, which is this guide's advice, not the FCC's: keep a **second way to reach 911**, such as a landline or a phone on another carrier.

Prescriptions

A pharmacy can be open and stocked and still unable to process the insurance claim. In **February 2024** a ransomware attack on Change Healthcare left pharmacies, hospitals and doctors unable to

submit insurance claims. UnitedHealth Group reported on **22 April 2024** that **99%** of pre-incident pharmacies could process claims again.

Ready.gov: "About half of all Americans take a prescription medicine every day." The **FDA** advice:

- "Keep a copy of your prescriptions with your emergency supplies."
- "If you expect your access to a pharmacy to be disrupted, obtain early refills."
- "learn about your state's emergency refill laws."

Ready.gov asks for a "Several days supply", no number. The only current CDC day count verified for this guide, "at least 7 days", is on a page written for cancer survivors.

For refrigerated drugs, Ready.gov says: "If the power is out for more than a day, discard any medication that should be refrigerated, unless the drug's label says otherwise." For insulin the FDA says it "may be left unrefrigerated at a temperature between 59°F and 86°F for up to 28 days." Check your own label.

Uninsured people in an area where it is activated can get "a free 30-day supply" through the federal **Emergency Prescription Assistance Program**. It is not activated everywhere. Hotline: **1-855-793-7470**.

Fuel

Gas stations need fuel and electricity. On **7 May 2021** a ransomware attack by the criminal group DarkSide led Colonial Pipeline to shut down "all **5,500** miles of pipelines," which carry "nearly half of the fuel consumed on the East Coast." Restart began on **12 May**. Colonial's chief executive told the Senate of "panic-buying and shortages on the East Coast." Ready.gov adds: "Gas stations rely on electricity to power their pumps."

Ready.gov's advice is a standing habit: "Keep a half tank of gas in it at all times in case of an unexpected need to evacuate," and a full tank "if an evacuation seems likely."

Water

Water utilities run on computer controllers that attackers have reached. In **November 2023** CISA reported that attackers likely got into a controller at a U.S. water facility through "poor password security and exposure to the internet." The water authority "switched to manual operations," with "no known risk" to the drinking water. In **July 2026** CISA observed activity targeting "more than 100" water and wastewater entities, with no official attribution. No official report of unsafe tap water from these incidents was found.

Ready.gov names the household risk: "Your regular water source could be cut-off or compromised through contamination." It says to "Store at least one gallon of water per person per day for several days." The **CDC** gives a number: "for 3 days," and "Try to store a 2-week supply if possible." Chapter 1 has the gallons for your household.

Grocery refrigeration and the fridge at home

A home fridge keeps food safe for **up to 4 hours** without power, if the door stays closed. In **October 2026** attackers pushed refrigerators at about **700** French supermarkets to **50°C (122°F)** for about six hours, and stores threw out fresh and frozen food (AP). France has blamed a unit of Iran's Revolutionary Guard; Iran calls the accusation "baseless and biased." No such attack on U.S. grocery refrigeration was found.

At home, **FoodSafety.gov** sets the clock:

- Fridge: safe "for up to 4 hours." After that, discard meat, poultry, fish, eggs and leftovers.
- Freezer: "A full freezer will hold a safe temperature for approximately 48 hours (24 hours if it is half full and the door remains closed)."
- Never taste food to check it.

Ready.gov adds: "Throw out food if the temperature is 40 degrees or higher." That takes a thermometer in the fridge and the freezer.

Gear for this step
Fridge and freezer thermometers, and a cooler for when the outage passes 4 hours. Our gear list names what Ready.gov asks for, with what each item does at home. **See the gear list →**

From the 72-Hour Readiness Kit
The Outage Cheat Sheets put the fridge and freezer keep-or-toss rules on one laminate-ready card, so the answer is on the fridge door before the power goes out. **See the kit, $27 →**

Apps and the cloud

Apps, email and cloud files run on other people's servers. On **19 and 20 October 2025** a latent defect in Amazon Web Services' own DNS automation disrupted its main U.S. region for **14 hours 32 minutes** (worked out from the start and end times in AWS's summary). In November 2026 Outlook and Teams went offline worldwide; Microsoft said it was not a cybersecurity breach.

Ready.gov: "Back up your files regularly in an encrypted file or encrypted file storage device." For documents it lists "a safety deposit box, an external drive or on the cloud." An outage takes the cloud away, so this guide adds a paper copy of the essentials. That is this guide's advice, not Ready.gov's. Chapter 6 builds the paper kit.

Do this now

- [ ] Keep small bills at home
- [ ] Check the FCC's text-to-911 list for your area, and keep one corded phone or a second carrier
- [ ] Ask your pharmacist about early refills and your state's emergency refill law
- [ ] Refill the car at a **half tank**, not at empty

- [ ] Put a thermometer in the fridge and the freezer
- [ ] Copy prescriptions and key documents onto paper

Chapter 6: The Offline Backup Kit



An offline backup kit is five things that work with the power and the network down: **cash in small bills**, **copies of your cards**, **printed account recovery codes**, a **downloaded map**, and **paper lists** of phone numbers and medicines. Each one replaces something your phone or a server normally holds for you. Ready.gov, the FDIC, the FCC, the FDA, Google, Apple and Microsoft each recommend a piece of it.

This chapter puts the pieces in one place. Chapter 5 covers why each one fails.

Cash in small bills, and copies of your cards

Keep a small amount of cash at home, in small bills. **Ready.gov** gives the reason: "It is important to have small bills on hand because ATMs and credit cards may not work during a disaster when you need to purchase necessary supplies, fuel or food." Its power-outage page adds that an outage can "Close retail businesses, grocery stores, gas stations, ATMs, banks and other services."

The **FDIC** (August 2025) says the same thing in its own words: keep "a small amount of cash to purchase food or supplies, in case ATMs and credit cards are not working." Neither page puts a dollar figure on "small." That amount is yours to set.

The FDIC adds a second item. It lists "Copies of your financial information such as credit and debit cards (**front and back**) and checks (**front**). During a disaster, you may need this information to authorize payments."

Ready.gov tells households to store important documents "either in a safety deposit box, an external drive or on the cloud." A cloud copy needs the internet to open. Keeping a **paper copy** as well is this guide's advice, not Ready.gov's. Store the card copies with the cash, in what Ready.gov calls "a safe place."

Printed backup and recovery codes

Google, Apple and Microsoft each tell you to print your account recovery code. The U.S. government doesn't: CISA's multifactor pages and the FTC's two-factor article say nothing about backup codes, so the advice here comes from the companies.

The codes matter when your phone is lost, broken or dead and two-step sign-in can't reach it:

Company	What you get	Where it says to keep it	What makes your copy useless
Google	A set of **10** backup codes, each usable **once**	Printed, "like where you keep your passport or other important documents"	Making a new set: "the old set automatically becomes inactive"
Apple	A **28-character** recovery key	"print a copy of your recovery key or write it down"	Losing it: "Apple can't provide you with your recovery key"
Microsoft	A **25-digit** recovery code	"Print the recovery code and keep it in a safe place"	Making a new one: "any previous codes will no longer work"

Three rules follow from that table, all from the companies' own pages:

- **Keep the code off the device it protects.** Microsoft: "do not store the code on a device used to sign in to your account." Apple: don't store the key in "your Apple Passwords app, iCloud Photos, Notes, or iCloud Drive," because "If you lose access to your Apple Account, you won't be able to open these apps to find it."
- **Reprint after every reset.** Google and Microsoft both cancel the old code when you make a new one. A sheet printed last year may already be dead.
- **Cross off used Google codes.** Each works once, and Google suggests you "mark the code as used."

Apple also offers a person instead of a code. A recovery contact "should be a person that you know and trust," and you can add "up to **five** recovery contacts."

Chapter 7 covers a related lock: the FBI's advice never to give a two-factor code to anyone.

Offline maps, and where they stop working

Google Maps lets you save an area to your phone and "use it when you're offline." The limits are the part to know before you rely on it.

- **The whole trip has to fit.** Offline maps "can guide you to your destination as long as the entire route is within the offline map." Download an area large enough to cover the drives you'd actually make in an emergency, not only your own street.
- **Driving only.** "When you're offline, transit, bicycling, or walking directions are unavailable." You also lose "traffic info or alternate routes."
- **The map expires.** "You must update the offline maps you've downloaded on your phone or tablet before they expire." Google tries to update an area automatically when it is within **15 days** of expiring and the phone is "connected to Wi-Fi."

Google's help page doesn't say how long an offline map lasts before it expires. The automatic update needs Wi-Fi, so refresh the map while the network is still up.

Phone numbers on paper, and one contact out of the area

Ready.gov Kids tells families to "write down your contacts and plans. Make sure everyone in the family has copies and keeps them in a safe space, like in a backpack, wallet, or taped in a notebook. Put them in your cell phone if you have one."

The Ready.gov and FEMA Family Emergency Communication Plan goes further: "create a paper copy of the contact information for your family and other important people/offices, such as medical facilities, doctors, schools, or service providers." Ready.gov's Make a Plan page links a fillable card for this.

The **FCC** adds the out-of-area contact: "Designate someone out of the area as a central contact, and make certain all family members know who to contact if they become separated." This guide's version of the paper list holds:

- **Each household member's** cell number
- **The out-of-area contact**, with a second number if they have one
- **Doctors, pharmacy, schools and workplaces**
- **Your bank and card issuers**, the numbers you need if the card copies come into play

Chapter 5 covers what to do when calls fail and texts get through.

The written medication list

"About **half of all Americans** take a prescription medicine every day," says **Ready.gov**, and an emergency "can make it difficult for them to refill their prescription or to find an open pharmacy." A paper list lets a new pharmacy or doctor see what you take without reaching your records.

The **FDA** and Ready.gov each say what goes on the list. Combined, one line per medicine holds:

Field	FDA	Ready.gov
Name of each medicine	"name"	"A list of all medications"

Strength and amount	"strength", "how much you take"	"dosage"
When you take it	"when"	"frequency"
What it is for	"what it is for"	not listed
Medical conditions	"medical conditions"	"diagnosis"
Medical supply needs	"medical supply needs"	"medical supply needs"
Allergies	"allergies"	"allergies"

Then add the paper prescription itself. The FDA: "Keep a copy of your prescriptions with your emergency supplies."

Both sources leave the day count to you. Ready.gov's kit list says "Several days supply of prescription medicines," and the FDA page gives no number. Chapter 5 covers early refills and your state's emergency refill laws.

From the 72-Hour Readiness Kit
The Digital Blackout Kit and the Family Emergency Binder turn this chapter into fill-in pages: cash, recovery codes, offline maps, phone numbers and the medication list, set up in one weekend. **See the kit, $27 →**

Do this now

- [ ] Withdraw a stack of small bills and store it at home with photocopies of your cards (front and back) and a check (front)
- [ ] Print the Google backup codes, the Apple recovery key and the Microsoft recovery code for every account that uses them, and file them with your important papers
- [ ] Download an offline Google Maps area that covers every route you'd drive in an emergency, and update it whenever you're on Wi-Fi
- [ ] Write a contact list with every household number, one out-of-area contact, doctors, pharmacy and schools; give each person a copy
- [ ] Write one line per medicine (name, strength, purpose, dose, timing, conditions, supplies, allergies) and put a copy of each prescription with it

Chapter 7: Crisis Cyber Hygiene and Your 72-Hour Plan



Two habits protect a household when systems fail: **CISA's four core steps** for every account and device, and a supply plan that covers **72 hours** at the least and **one week** as the goal. A family of four needs **12 gallons** of water for the first and **28 gallons** for the second, at Ready.gov's rate of **1 gallon per person per day**.

The cyber steps come first because they need no supplies. The supplies take longer, so the second half of this chapter turns them into a list and a clock.

The four steps CISA asks of everyone

The **Cybersecurity and Infrastructure Security Agency (CISA)** puts its household advice in one line: "Everyone should take these 4 core steps." In CISA's order and wording, they are:

1. **"Avoid and report phishing scams."**
2. **"Use strong passwords."**
3. **"Use multifactor authentication and a password manager."**
4. **"Update software."**

In CISA's list, phishing comes first, and CISA pairs the password manager with multifactor authentication (MFA), not with passwords. On MFA, CISA's reasoning is short: "Even if an unauthorized user steals your password, they won't be able to meet the second step requirement to access your accounts."

Ready.gov's cybersecurity page, last updated **February 20, 2026**, adds four habits that fit beside CISA's list:

- "Back up your files regularly in an encrypted file or encrypted file storage device."
- "Keep software applications and operating systems up-to-date."
- "Check your account statements and credit reports regularly."
- "Do not click on links in texts or emails from people you don't know."

It also gives a rule worth taping to the fridge: "the government will not call, text or contact you via social media about owing money." Chapter 4 covers the scams that follow a crisis, including fake disaster aid.

What to do if an account or device is hit

Ready.gov gives the steps in two stages: limit the damage now, then report it.

When	Ready.gov says
You notice strange activity	"limit the damage by changing all of your internet account passwords immediately"
You find a problem on a device	"disconnect your device from the Internet and perform a full system restore"
Afterward	"Contact banks, credit card companies and other financial services companies where you hold accounts"
Afterward	"File a complaint with the FBI Internet Crime Complaint Center (IC3)" and "Report identity theft to the Federal Trade Commission"

For a device, Ready.gov's order is to disconnect it from the internet first, then restore it.

Two locks that cost nothing

Never give a two-factor code to anyone. The FBI's IC3 put it plainly in a **May 2025** public service announcement about criminals impersonating senior U.S. officials with texts and AI-generated voice messages: "Never provide a two-factor code to anyone over email, SMS/MMS text message or encrypted messaging application." The code is the second lock. A caller who asks for it is asking for the key. The same announcement tells families to "Create a secret word or phrase with your family members to verify their identities."

Freeze your credit. The **Federal Trade Commission (FTC)** says of a credit freeze: "When in place, it prevents potential creditors from accessing your credit report." It also says "Placing and lifting the

freeze is free." To set one up, "Place a credit freeze by contacting each of the three national credit bureaus." That's **three** separate requests, one per bureau. This guide's reasoning: a freeze set before a crisis is one less thing to do during it.

Printing your account recovery codes belongs with these two. Chapter 6 covers that, along with cash and offline maps.

The plan: 72 hours as the floor, a week as the goal

This guide sets **72 hours as the floor and one week as the goal**, as Chapter 1 explains. That's the guide's own choice. Ready.gov asks for "several days" and names no number; the **CDC** says "Store at least 1 gallon of water per person, per day for 3 days" and adds "Try to store a 2-week supply if possible."

Water is the first number to get right. Ready.gov's gallon covers "drinking and sanitation." The **UK** and **Japan** count differently, at **3 litres** per person per day for drinking (Japan includes water for cooking).

Household of 4	72 hours	One week
Gallons needed	**12**	**28**
24-packs of 16.9-oz bottles	**4**	**9**

Worked out as 4 people × 1 gallon × days; each 24-pack holds 24 × 16.9 oz = 405.6 oz, or 3.17 gallons, so 28 ÷ 3.17 = 8.8, rounded up to 9 cases.

Three adjustments from Ready.gov and the CDC:

- **Double it in heat.** Ready.gov: "In very hot temperatures, water needs can double."
- **Rotate it.** CDC: "replace the water every 6 months" if you filled the containers yourself.
- **Drink it.** Ready.gov: "Never ration drinking water unless ordered to do so by authorities."

> **Gear for this step**
> Water containers: 12 gallons for a family of four is 3 five-gallon containers, and 28 gallons is 6.
>
> Our gear list shows the math and what to buy. **See the gear list →**

The first 72 hours, hour by hour

The sources behind this guide give clock times, not a schedule. The schedule below hangs official advice on the clock times the agencies do give: **4 hours** for the fridge, **24** and **48 hours** for the freezer, and **one day** for refrigerated medicine.

Hour 0: the power goes out.

- Light the house with flashlights. The Red Cross says "Use flashlights, not candles," and Ready.gov says "Have flashlights for every household member."

- "Disconnect appliances and electronics to avoid damage from electrical surges" (Ready.gov).
- Keep the fridge and freezer doors shut.
- Text instead of calling. The FCC says "In many cases text messages will go through when your call may not," and to "Wait 10 seconds before redialing a call."
- Switch your phone "to low power mode or place it on airplane mode to conserve energy" (Ready.gov).
- Run any generator outside, "more than 20 feet away from windows, doors, and vents." The CDC says "Never use a generator inside your home or garage, even if doors and windows are open."

Hours 1 to 4: eat from the fridge.

- "Eat your fresh, perishable foods first" (Red Cross).
- At **4 hours**, FoodSafety.gov says to "Discard refrigerated perishable food such as meat, poultry, fish, eggs, and leftovers after 4 hours without power."

Hour 24: check the freezer and the medicine.

- A half-full freezer holds a safe temperature for about **24 hours** with the door closed (FoodSafety.gov).
- Ready.gov: "If the power is out for more than a day, discard any medication that should be refrigerated, unless the drug's label says otherwise. Consult your doctor or pharmacist immediately for a new supply."
- "Check on family members, older adults and neighbors" (Ready.gov).

Hour 48: the full freezer's limit.

- A full freezer holds for about **48 hours** (FoodSafety.gov). The CDC says "You can safely refreeze or cook thawed frozen food that still contains ice crystals or is at 40 °F or below."
- "Never taste food to know if it is safe to eat. When in doubt, throw it out" (CDC).

Hour 72: the floor.

- A household of four has used **12 gallons** of water at Ready.gov's rate.
- "Go to a community location with power if heat or cold is extreme" (Ready.gov). FEMA's shelter search works by text: "Search for open shelters by texting SHELTER and your ZIP code to 43362."

Through all three days, keep camp stoves, charcoal and generators out of the house. The CDC says "Never use a portable gas camp stove indoors," "Never burn charcoal indoors" and "Never heat your house with a gas oven." Chapter 5 covers what else fails at home over those days: cards, fuel, prescriptions and the phone network.

Gear for this step
A flashlight for each person, spare batteries in the right size, a hand-crank weather radio, a phone backup battery and a carbon monoxide alarm with battery backup on every level. Our gear list covers all 9 items, each with the Ready.gov line behind it. **See the gear list →**

From the 72-Hour Readiness Kit
The 30-Day Prep Plan breaks this plan into one small task a day, and the 72-Hour Apartment Prep Checklist lists every supply and number for 3 days. **See the kit, $27 →**

Do this now

- [ ] Turn on multifactor authentication for your email and bank accounts, and install system updates
- [ ] Back up your files to an encrypted drive tonight
- [ ] Place a credit freeze with each of the **three** national credit bureaus
- [ ] Agree on a family code word, and agree that nobody reads out a two-factor code to anyone
- [ ] Store **3 gallons** of water per person now, then build to **7**
- [ ] Copy the hour-by-hour list above and tape it inside a kitchen cabinet

Sources

Every fact in this guide comes from the sources below, listed by chapter.

Chapter 1: Why Governments Now Say 72 Hours, or a Week

- Estonian Rescue Board, crisis instructions mailing (5 July 2024): rescue.ee; *Ole valmis!* guide (2022): kriis.ee
- Denmark, Beredskabsstyrelsen, "Forberedt på kriser" (15 June 2024): brs.dk; Styrelsen for Samfundssikkerhed campaign (24 November 2025): samsik.dk
- Norway, DSB, egenberedskap brochure (2024): dsb.no/egenberedskap
- Sweden, MSB/MCF, *Om krisen eller kriget kommer* (2024): mcf.se
- Finland, "Preparing for incidents and crises" (18 November 2024): suomi.fi
- European Commission, Preparedness Union Strategy (26 March 2025): commission.europa.eu
- Poland, *Poradnik bezpieczeństwa* (2025): sop.gov.pl
- Germany, BBK, household supplies guidance: bbk.bund.de
- Netherlands, Rijksoverheid, "Denk vooruit" campaign (3 November 2025): rijksoverheid.nl; denkvooruit.nl
- United Kingdom, Cabinet Office, "Be Ready" (22 October 2026): gov.uk
- Japan, Cabinet Office, Disaster Management Minister's urgent request (2 November 2026): bousai.go.jp
- Ready.gov, "Build a Kit" (updated 1 July 2026) and "Water": ready.gov/kit, ready.gov/water
- The White House, "Achieving Efficiency Through State and Local Preparedness" (18 March 2025): whitehouse.gov
- FEMA Review Council, final report (approved 7 May 2026): dhs.gov

Chapter 2: The Outage Record

- FCC Public Safety and Homeland Security Bureau, *February 22, 2024 AT&T Mobility Network Outage Report and Findings* (22 July 2024): docs.fcc.gov
- FCC, public notice DA 26-94 on the Verizon outage (28 January 2026): docs.fcc.gov
- Verizon statement on the cause, as reported by Mashable
- CrowdStrike, "Falcon update for Windows hosts: technical details" (July 2024): crowdstrike.com
- Microsoft, "Helping our customers through the CrowdStrike outage" (20 July 2024): blogs.microsoft.com
- FAA, NOTAM statements (January 2023): faa.gov
- ENTSO-E, "28 April 2025 Iberian blackout": entsoe.eu
- Euronews, "Spain says April's blackout was caused by multiple technical failures and rules out cyberattack" (17 June 2025): euronews.com
- Amazon Web Services, post-event summary for the us-east-1 event (October 2025): aws.amazon.com/message/101925
- CNN, Microsoft 365 outage report (12 November 2026, updated 13 November): cnn.com
- Colonial Pipeline, testimony of CEO Joseph Blount to the Senate Homeland Security and Governmental Affairs Committee (8 June 2021): hsgac.senate.gov
- CISA, "The Attack on Colonial Pipeline: What We've Learned and What We've Done Over the Past Two Years": cisa.gov
- HHS, statement on the cyberattack on Change Healthcare (5 March 2024): hhs.gov
- UnitedHealth Group, update on the Change Healthcare cyberattack (22 April 2024): unitedhealthgroup.com
- Fierce Healthcare, UnitedHealth estimate of people affected (January 2025): fiercehealthcare.com
- FlightAware counts for 11 January 2023, as reported by the press
- Ready.gov, "Financial Preparedness": ready.gov/financial-preparedness
- FDA, "Safe Drug Use After a Natural Disaster": fda.gov

Chapter 3: How AI Changes the Attacks on Power, Water and Food

- ASD/ACSC, CCCS, GCSB/NCSC-NZ, NCSC-UK, NSA and CISA, *The AI shift in cyber risk: why leaders must act now* (22 June 2026): cyber.gc.ca; ncsc.gov.uk
- NSA, CISA, FBI, DOE and EPA, advisory AA26-231A, *Defending Against an Active Threat to Siemens S7 Series PLCs* (19 August 2026): cisa.gov
- DOE/DHS, *Section 2(e): Assessment of Electricity Disruption Incident Response Capabilities* (9 August 2017): energy.gov
- CISA, ICS alert IR-ALERT-H-16-056-01, and CISA, FBI and NSA, advisory AA22-011A: cisa.gov
- PCWorld, Kyiv outage restoration time from Ukrenergo (20 December 2016): pcworld.com
- CISA, NSA and FBI, advisory AA24-038A (Volt Typhoon) (7 February 2024): cisa.gov
- EPA, Enforcement Alert: drinking water systems and cybersecurity vulnerabilities (May 2024): epa.gov
- CISA, alert on exploitation of Unitronics PLCs in water and wastewater systems (28 November 2023): cisa.gov
- CISA, EPA and FBI, "Top Cyber Actions for Securing Water Systems" (23 February 2024): cisa.gov
- CISA, "Internet Exposure Reduction Guidance" (revised 21 August 2026): cisa.gov
- AP via ABC News, France blames Iran for supermarket fridge cyberattack (9 November 2026): abcnews.com; franceinfo, Paris prosecutor (November 2026): franceinfo.fr
- France 24 with AFP and Reuters, Barrot on the IRGC (9 November 2026): france24.com
- AP via PBS (2 November 2026): pbs.org; Reuters via Devdiscourse, Axfood (2 November 2026): devdiscourse.com
- ENISA, European Commission DG CNECT and Europol EC3, joint statement (4 November 2026): enisa.europa.eu
- Ready.gov, "Water" and "Power Outages": ready.gov
- CDC, "How to Create and Store an Emergency Water Supply" (27 June 2025): cdc.gov
- FoodSafety.gov, "Food Safety During a Power Outage" (reviewed 8 August 2024): foodsafety.gov

Chapter 4: How AI Changes the Scams That Follow a Crisis

- FBI, IC3, *2025 Internet Crime Report* (2026), AI section and 60+ tables: ic3.gov
- FBI, IC3, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud" (3 December 2024): ic3.gov
- FBI, IC3, "Senior US Officials Impersonated in Malicious Messaging Campaign" (15 May 2025): ic3.gov
- FBI, IC3, "Scammers Impersonating Law Enforcement and Government Officials in Fraud Schemes" (17 September 2026): ic3.gov
- FTC, "Scammers use AI to enhance their family emergency schemes" (20 March 2023): consumer.ftc.gov
- FTC, prepared statement to the Joint Economic Committee, "The Rising Scam Economy" (25 March 2026): ftc.gov
- FTC, press release on 2025 imposter-scam losses (15 June 2026): ftc.gov
- FCC, Declaratory Ruling FCC 24-17, CG Docket No. 23-362 (adopted 2 February 2024, released 8 February 2024): docs.fcc.gov
- FTC, "Spot and avoid FEMA impersonators" (14 July 2025): consumer.ftc.gov
- FTC, "Recovery scams will follow Hurricane Helene. Here's how to spot them" (1 October 2024): consumer.ftc.gov
- FTC, DOJ and CFPB, joint warning on scams after the hurricanes (9 October 2024): ftc.gov
- FEMA, "Beware of Fraud and Scams," DR-4893-AK (4 December 2025); "Be Alert to Fraud After Washington Storms and Flooding" (23 April 2026); "Disaster Fraud" (updated 26 June 2026): fema.gov
- FEMA, "Common Disaster-Related Rumors" (updated 25 June 2026) and "Hurricane Rumor Response": fema.gov
- CISA, "Avoid Scams After Disaster Strikes" (8 October 2024, revised 26 January 2026): cisa.gov
- DHS Science and Technology Directorate, "Impacts of Adversarial Use of Generative AI on Homeland Security" (January 2025): dhs.gov

Chapter 5: What Fails at Home When the Systems Go Down

- CrowdStrike, Falcon update technical details (July 2024): crowdstrike.com; Microsoft, "Helping our customers through the CrowdStrike outage" (20 July 2024): blogs.microsoft.com
- Ready.gov, "Financial Preparedness" (13 March 2026), "Power Outages" (4 June 2026), "Build a Kit" (1 July 2026), "People with Disabilities" (9 September 2026), "Evacuation" (20 March 2026), "Space Weather" (5 March 2026),

"Cybersecurity" (20 February 2026), "Water" (22 February 2021): ready.gov
- FDIC, "Preparing Your Finances for an Unanticipated Disaster" (August 2025): fdic.gov
- FCC, AT&T Mobility Network Outage Report (22 July 2024), "Tips for Communicating in an Emergency" and "Text to 911" (reviewed 6 January 2020): fcc.gov
- HHS statement on Change Healthcare (5 March 2024): hhs.gov; UnitedHealth Group (22 April 2024): unitedhealthgroup.com
- FDA, "Safe Drug Use After a Natural Disaster" (1 September 2026) and insulin storage guidance: fda.gov
- CDC, "Be Prepared for an Emergency" (17 April 2026) and emergency water supply (27 June 2025): cdc.gov
- HHS/ASPR, Emergency Prescription Assistance Program: aspr.gov
- Colonial Pipeline, Joseph Blount Senate testimony (8 June 2021): hsgac.senate.gov
- CISA, Unitronics PLC alert (28 November 2023) and Internet Exposure Reduction Guidance (21 August 2026): cisa.gov
- AP via ABC News (9 November 2026): abcnews.com; France 24 (9 November 2026): france24.com
- FoodSafety.gov, "Food Safety During Power Outage" (8 August 2024): foodsafety.gov
- AWS, post-event summary (October 2025): aws.amazon.com
- CNN, Microsoft 365 outage (12 November 2026): cnn.com

Chapter 6: The Offline Backup Kit

- Ready.gov, "Financial Preparedness" (updated 13 March 2026): ready.gov/financial-preparedness
- Ready.gov, "Power Outages" (updated 4 June 2026): ready.gov/power-outages
- FDIC Consumer News, "Preparing Your Finances for an Unanticipated Disaster" (August 2025): fdic.gov
- Google Account Help, backup codes: support.google.com/accounts/answer/1187538
- Apple Support, recovery key (published 14 September 2026): support.apple.com/en-us/109345; recovery contacts: support.apple.com/en-us/102641
- Microsoft Support, recovery code: support.microsoft.com/en-us/accounts-billing/manage/how-to-get-a-microsoft-account-recovery-code
- Google Maps Help, "Download areas & navigate offline in Google Maps": support.google.com/maps/answer/6291838
- Ready.gov Kids, "Make a Plan" (updated 29 April 2026): ready.gov/kids/make-a-plan
- Ready.gov, "Make a Plan" (updated 1 September 2026): ready.gov/plan
- Ready.gov and FEMA, Family Emergency Communication Plan (hosted copy at mssp.uscourts.gov; Ready.gov says the plan is being revised)
- FCC, "Tips for Communicating in an Emergency": fcc.gov
- Ready.gov, "Build a Kit" (updated 1 July 2026): ready.gov/kit; "People with Disabilities" (updated 9 September 2026): ready.gov/people-disabilities
- FDA, "Safe Drug Use After a Natural Disaster" (current as of 1 September 2026): fda.gov
- CISA, multifactor authentication page: cisa.gov
- FTC, "Use Two-Factor Authentication to Protect Your Accounts" (September 2022): consumer.ftc.gov

Chapter 7: Crisis Cyber Hygiene and Your 72-Hour Plan

- CISA, "Secure Our World" and its multifactor authentication page: cisa.gov
- Ready.gov, "Cybersecurity" (updated 20 February 2026): ready.gov/cybersecurity
- FBI Internet Crime Complaint Center, PSA "Senior US Officials Impersonated in Malicious Messaging Campaign" (15 May 2025): ic3.gov
- Federal Trade Commission, "Is a credit freeze or fraud alert right for you?": consumer.ftc.gov
- Ready.gov, "Build a Kit" (updated 1 July 2026), "Water" (updated 22 February 2021), "Power Outages" (updated 4 June 2026), "Get Tech Ready" and "Heat": ready.gov
- CDC, "How to Create and Store an Emergency Water Supply" (27 June 2025), food safety after an emergency and "Carbon Monoxide Poisoning Basics": cdc.gov
- FoodSafety.gov, "Food Safety During Power Outage" (reviewed 8 August 2024): foodsafety.gov
- FCC, "Tips for Communicating in an Emergency": fcc.gov

- American Red Cross, "Power Outage": redcross.org
- FEMA, "How do I find emergency shelter near me?": fema.gov
- UK Cabinet Office, "Be Ready" (22 October 2026): beready.campaign.gov.uk; Japan Cabinet Office, Urgent Request (2 November 2026): bousai.go.jp

Your Next Step

You now know what governments are asking for, what has already failed and what to do about it. The hard part is doing it before the next outage, with the right numbers in front of you when the lights are off.

That's what the **72-Hour Readiness Kit** is for. It turns this guide into things you print, fill in and keep with your flashlights.

In the kit	What it does
The 72-Hour Apartment Prep Checklist (12 pages)	Every supply, every number, for three days without power or water
The Outage Cheat Sheets (9 cards)	One page each for the first hour, the fridge, water, carbon monoxide, heat and cold illness, phones and radio, cash and paper, the bucket toilet, and AI scams. Laminate them.
The Family Emergency Binder (12 pages)	Fill-in pages for contacts, medications, documents, shutoffs, school pickup, pets and an outage log
The Digital Blackout Kit (9 pages)	Cash, phones and 911, medicine, fuel, account recovery and offline maps, ending with a one-weekend setup
The 30-Day Prep Plan (5 pages)	One small task a day, each pointing to the page that explains it

New guides are added to the kit as they're written, at no extra cost to anyone who already has it.

$27, one time. Try the whole kit for 30 days. If it isn't worth $27 to you, email us and get every cent back, no questions asked.

Get the 72-Hour Readiness Kit at prepnskills.com