REVEALRISK

Family Cyber Incident Response Plan

How our household will prepare for, respond to, and recover from cyber incidents such as identity theft, online fraud/scams, or device compromise.

Roles and Responsibilities

Key Roles	Responsibility
1. Designated Family Member	The Designated Family Member is the primary decision maker and is responsible for keeping this plan up to date. They will receive support and input from all family members, but will ultimately make decisions. They will also be the first point of contact if something happens.
2. Technology Expert (in or outside the family)	The Technology Expert will be responsible for providing technical support to family members impacted by a cyber issue. This person should be comfortable with technology.

Tip: choose someone non-judgmental, calm, and tech-savvy if possible!

Tip: find someone non-judgmental and comfortable with doing things like installing software!

Preventative Actions

Follow these tips to avoid common cyber scams.

- **Verify a request with the sender or caller!** Got an urgent call from a bank, the IRS, or your boss? You can always hang up and call them back. If it's not expected, confirm it.
- There are no scenarios where a company will call you and ask you to download software. This is an easy way for someone to get remote access to your computer.

- Only download apps from reputable sources like the **Google Play Store or Apple App Store,** not random websites or links on social media, ads, or emails.

- **Pause & discuss urgent or unexpected requests.** Remind everyone, especially kids and elders, not to act on urgent calls or emails without using the family code phrase.

- **Update devices and software promptly** to fix known security flaws.

- **Create unique, strong passwords for each online account**. Skip the options you're going to forget or want to reuse and go with long, memorable pass phrases instead!

- Consider using a **password manager** that will generate unique, strong passwords for each account, remember them for you, and automatically fill them in when logging in.

- **Enable two-factor authentication** on all your accounts where available, but especially email, bank, and social accounts. One-time codes can save you a lot of hassle!

- Don't click on links or download attachments from **unknown or unexpected senders.**

- **Establish a code word and/or phrase with your loved ones**—and write it in the template! Families can decide together when to use their code word and should agree never to share it with anyone outside the family. Whenever someone receives a call, text, or message—especially if the situation feels *urgent, secretive, or someone is making demands or claiming to be in trouble*—pause and calmly **ask them to say the code word**.

An Action Plan for When a Cyber Mistake Happens

It's okay! These things happen to everyone—really.

Step 1: STOP, BREATHE, and FOCUS

First things first: take a couple of *big, deep breaths*.

1. **Disconnect immediately.** Hang up the phone or turn off the Wi-Fi. For a cell phone, turn on Airplane Mode. This cuts off the bad guys and prevents more damage. To preserve potential evidence, leave your devices on and plugged in.
2. **Do not engage.** If possible, don't reply to the email, text, or caller. If you haven't already, don't pay any money, even if someone threatens you.
3. **Take a screenshot.** If you can, take a screenshot or photo of the message, link, or anything else that seems suspicious.
4. Contact your **designated family member**.

Step 2: ASSESS THE SITUATION

Something is definitely wrong... What happened?

1. Determine what information or assets have been involved.
2. If you're feeling shaken up, **write down your answers** so you can keep them straight.
   - Did the situation make you feel **worried, scared, under pressure,** or something else?
   - Did you enter a **password**? If so, which account was it for?
   - Did you **download a file**? If so, what was the file name?
   - Did you **send money or buy gift cards**? If so, how did you send the money?
   - Did you give someone **access** to your computer? How?
   - What information did you provide?
     - Examples: date of birth, password, social security number, personal health or insurance information, benefits information, bank account details.

Action Plan (Part 2)

Step 3: TAKE ACTION

If you entered a password:

1. **Change it immediately.** Go to the real website on a different, trusted device. Log in and change the password for that account right away.
2. **Check your other accounts.** If you use that same password anywhere else, go and change it on those sites too. PS: remember to change them to long and unique new passwords!

If you downloaded a file or suspect a virus:

1. **Disconnect from the internet**. If you already did this in Step 1, don't reconnect yet.
2. **Run an antivirus scan.** Use the antivirus software on your computer to run a full system scan. If you don't have one, get in touch with your technology expert and get help downloading a tool.

If you sent money or bought gift cards:

1. **Call your bank or credit card company.** Request that they reverse the transaction.
2. **Call the gift card issuer.** Call the number on the back of the gift card and report the scam.

Step 4: REPORT & RECOVER

1. **Report the scam.**
   - Reports can be made to law enforcement via non-emergency numbers.
   - You can also report the incident to the Federal Trade Commission (FTC) at ReportFraud.ftc.gov or the Internet Crime Compliant Center (IC3) at IC3.gov.
   - Reporting an incident helps law enforcement identify patterns and track down repeated scams. Even if they can't help with your individual problem, reporting can help others.
2. **Monitor your accounts.**
   - Notify your bank and credit card providers if financial impact is suspected.
   - Keep a close eye on your bank and credit card statements for any strange charges.
   - You may also want to set up a credit freeze.
3. **Learn... and share!**
   - *Remember: shame thrives in silence.* The best thing you can do is learn, tell your community about what happened, and help share cyber security tips with others.

OUR FAMILY CYBERSECURITY CONTACTS

1. Family Member in Charge of the Plan

Name: _____ Phone: _____

Relationship: _____ Email: _____

2. Other Key Contacts

Immediate Family:

Name: _____ Phone: _____

Name: _____ Phone: _____

Trusted Friend/Neighbor:

Name: _____ Phone: _____

Tech Expert Contact:

Name: _____ Phone: _____

3. Family Security Code Word/Phrase

Code Word: _____

Hint: _____

4. Financial Institution Contacts

Main Bank: _____ Phone: _____

Other Bank/Credit Card: _____ Phone: _____

5. Additional Contact Numbers

Local Police (non-emergency): _____

Internet Service Provider: _____

Attorney/Legal Aide: _____

6. **Important Online Accounts & Information**

Where are passwords kept? _____

Who has access to those passwords? _____

7. This space is for you to add any other **family-specific information** you might want to have on hand!