



5 WAYS TO PROTECT YOUR FAMILY FROM CYBER THREATS



Safeguard



Secure



Protect



Document



Educate

The Digital Battlefield

We all know cyber threats are real. Our identity could get stolen, our bank accounts hacked, and almost everyone has experienced a spam email trying to get you to click and enter your information. So how do you protect yourself and your family?

“Cyber warfare: computers used as weapons. It takes specially trained soldiers to fight and defend this digital battlefield,” says CBN Chairman, Pat Robertson. Individuals, and even entire governments, are using the internet to hack into various systems to take advantage of data from around the world.

“Counter terrorism experts say this is the new war,” says CBN News National Security Correspondent, Erik Rosales. *“Groups like ISIS may be losing territory on the battlefields of Iraq and Syria, but in cyberspace, it’s still going strong.”*

Here are 5 Ways to Protect Your Family from Cyber-Terrorism.



Safeguard Your Private Information

✓ Educate Your Family About Online Security

Once something is on the internet, it's online forever—even when it appears to have been deleted. Make sure your family understands this and never upload anything that wouldn't be wise to share with everyone.

✓ Create Complex Passwords & Update Regularly

The longer and more complex your passwords are, the harder they'll be for hackers to break. Each password should contain a mix of lowercase and uppercase letters, numbers, and symbols. **Experts recommend having a password that is 16 or more characters long.**

You should make sure all your passwords are different from one another and that you update them regularly.

✓ Set Up Two-Step Verification

Two-step verification helps protect you by making it more difficult for someone else to sign in to your accounts. If any of your accounts offer two-step verification, set it up immediately.

TWO STEP VERIFICATION:

Two-step verification uses two different forms of identity: your password, and a contact method (also known as security info).

✓ Adjust Privacy Settings

It is possible to make accounts like Twitter and Instagram private. For each account adjust the privacy levels to whatever makes you most comfortable. **Particularly on social media accounts, make sure you know who can see what you post.**



Secure Your Devices from Viruses & Malicious Software

✓ Never Open an Email or File From Someone You Don't Know

While your email filter is hopefully strong enough to sort out spam messages, don't assume that every email you receive is from a person who has honest intentions.

Read the email preview and if you're feeling uncertain or if it seems fishy, delete and do not open it.

✓ Consider Having Two Email Addresses

Sometimes getting info on the latest sales and news updates in your inbox creates a lot of clutter.

Consider having one email address for social and business interactions and a separate one you use for subscriptions and promotions.

✓ Update Your Devices

Software and computer companies are aware of vulnerabilities in their systems and often these updates are patches to fix them.

It's extremely important that you update all of your devices as soon as the update releases.

✓ Be Suspicious of Specific Things Online

Even if you receive an email from someone you know, their email account may have been compromised. Whenever you can, preview the following items:

- Email attachments
- Hyperlinks
- Items that require a download

MALWARE:

Short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms, Trojan horses, spyware, adware, and other malicious programs



Protect Yourself from Scams & Phishing

✓ Stop and Think

Before sharing any personal information, particularly banking information, stop, think, and ask yourself the following questions:

- Is this person/business legitimate?
- Why are they reaching out to you?
- Is this too good to be true?
- Should you check with the authorities before you give money or information to this person?

PHISHING:

Phishing occurs when an email appears to be from a trusted friend or company, but is actually a scam to steal information or take advantage of a victim.

✓ Don't Share Private Information with Anyone

Phishing can look like an e-mail that appears to be from your bank, or another trusted company, asking to confirm your account number or other personal information. Check the sender's email address to see if it looks suspicious and call the company or bank directly to confirm they sent the email before you submit any information.

A reputable company would never ask you to confirm personal information via email.

Things you should not share with anyone online unless you know it is safe:

- Your social security number
- Banking information
- Passwords
- Credit or debit card information
- Answers to commonly asked security questions (i.e. your mother's maiden name)



Document Your Information & Make a Plan

✓ **Keep a Record of Your Statements & Information**

Get into the habit of saving emails and statements from your financial institutions and creditors. While you do not need to print out every single document, consider backing up and periodically printing all your financial statements.

Make sure you know roughly how much money you have and owe at all times.

✓ **Create a “What If” Plan with Your Family**

If a massive cyber-terrorism attack were to occur and you were unable to use the internet or your phones, how would you know your family is safe?

Talk to your family about a plan and a meetup place if this were to take place.

“In the past six years, identity thieves have stolen over \$107 billion.”

- Insurance Information Institute

IDENTITY THEFT:

The fraudulent acquisition and use of a person’s private identifying information, usually for financial gain.

✓ **Consider Investing in Identity Theft Protection**

While there are many people who will never have their identity stolen, many choose to invest in identity theft protection the way they invest in insurance. There are a number of options to be found by doing an online search for “identity theft protection”.

Hopefully you’ll never need it, but it’s good to have just in case the worst should happen.



Educate Yourself About Networking & Security

✓ **Protect Your Home Network**

All of your devices are likely connected in your home and if someone can break into one, they can break into all of them.

Make sure you follow these steps to increase your network security:

- Change your wireless internet (wifi) network name -- use something that doesn't indicate your name or address.
- Choose a very strong and very unique network password.
- Use a wireless router with a firewall and make sure it is setup properly.

✓ **Be Aware of Cameras and Listening Devices**

If you have an Amazon Echo, Google Home, or any other device that talks to you, it is important to realize that it is always listening.

Also be aware that any cameras in your house -- security cameras, baby monitors, and computer cameras can be hacked into at any point.

Research your specific device to make sure that you're not being watched or listened to without you knowing it.

✓ **Clean Up Your Cookies**

Many websites you visit on a regular basis view your "cookies." If a website who views your cookies gets hacked, your information may be vulnerable. Use a search engine to find directions on clearing out cookies on your specific browser. **Get into the habit of regularly deleting or clearing out your cookies.**

COOKIES:

Tiny files that store data and can provide a lot of information to data hackers.

✓ **Do Not Use Public Wifi for Sensitive Information**

Even if you have to enter a password, the wifi at your doctor's office or local coffee shop is still a public network and your information is vulnerable.

While there is no 100% secure solution, taking these steps will help you keep your family safe in today's cyber world.

God is everywhere, even in the news.

**That's why we view every news story
through the lens of faith.**

**CBN News is committed to delivering
quality Christian journalism you can trust.
We are dedicated to honoring God's call on
our lives by bringing you the truth through
independent news coverage.**

**Follow along with us as we deliver
breaking updates on the latest in politics,
world news, Israel, health, entertainment,
and more - all from a Christian perspective.**

**CBN
NEWS**

