PEOPLE
TECHNOLOGY
A SAFER
TOMORROW

DON'T CLICK THAT

The PoeTech Global Survival Guide to Hackers, Scammers, AI Deception & Digital Self-Defense

Rev. Dr. Gerald F. Poe, Jr.

A POETECH GLOBAL BOOK

Copyright 2026 PoeTech Global.
All rights reserved.

Dedicated on behalf of the Poe Family Office
to all those who stand as defenders of God's people,
wheresoever dispersed.

"The prudent see danger and take refuge."

PROVERBS 22:3

KNOW MORE
STAY SAFER
LIVE FREER

STRONGER
PEOPLE
SAFER
COMMUNITIES

Table of CONTENTS

REAL KNOWLEDGE. A SAFER TOMORROW.

AWARENESS
PREVENTION
PROTECTION
EMPOWERMENT

1	Welcome and How to Use This Guide	4
2	Cybersecurity 101	12
3	AI 101 and Superintelligence 101	28
4	How Scammers and Hackers Really Attack	46
5	Protecting Your Phone	66
6	Protecting Your Computer and Home Network	86
7	Protecting Elders and Families	106
8	Protecting Youth Online	126
9	Spy Devices, Cameras, and Tracking	146
10	What To Do If You've Been Hacked	164
11	The Top 10 Rules for Personal and Work Safety	182



"Urgency is the attacker's weapon. Verification is yours."

SAME
PEOPLE
BIGGER
THREATS
SMARTER
YOU

Educational information only. Not legal advice.

ABOUT THE AUTHOR

FAITH • TECHNOLOGY • PEOPLE • A SAFER TOMORROW

Rev. Dr. Gerald F. Poe, Jr. is a technology and innovation leader, entrepreneur, minister, and public educator dedicated to a safer, more equitable digital future.

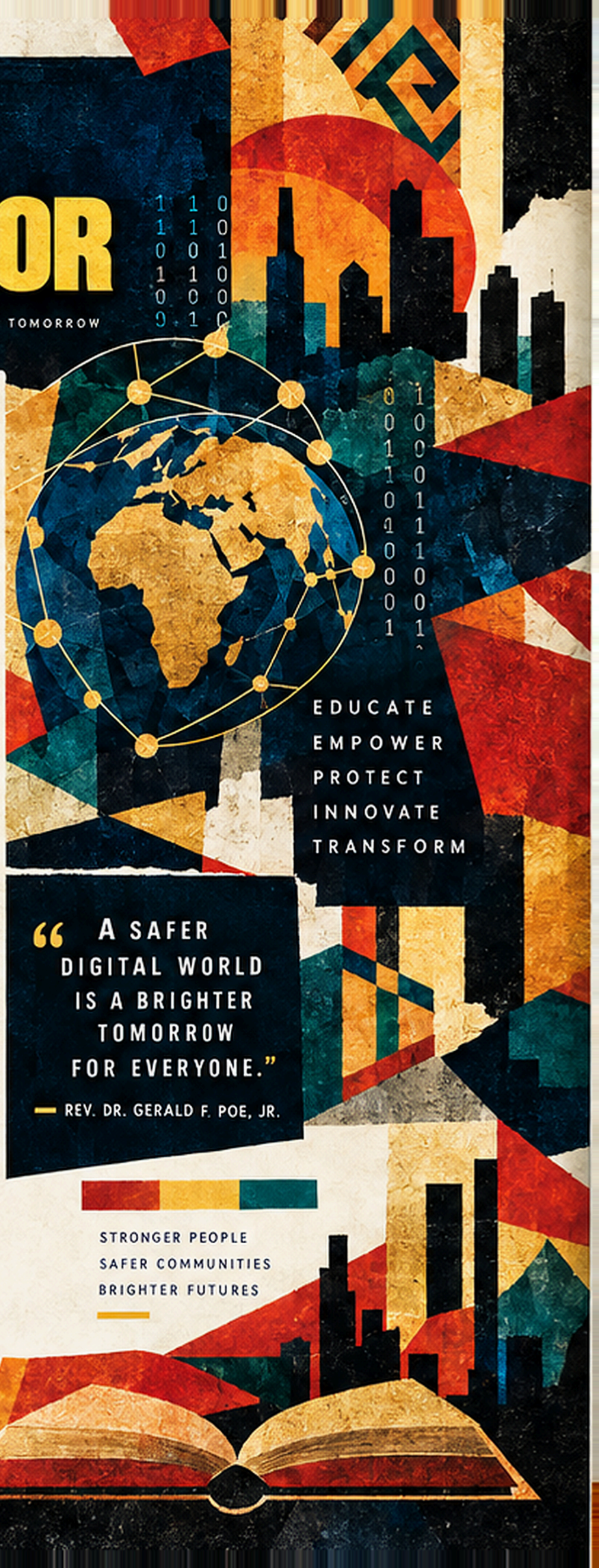
He is the founder of **PoeTech Global**, a technology education and advisory firm focused on cybersecurity awareness, AI literacy, and practical digital tools for everyday people, and the founder of Keystone Strategies International VC & Development, a venture and development company that supports innovative solutions at the intersection of technology, community, and human potential.

With more than 30 years of experience, Dr. Poe has led and supported initiatives across government, industry, and community sectors, including work associated with NASA, the U.S. EPA, the FDA, Tesla, and other modernization efforts. A veteran, he brings a unique blend of disciplined service, strategic insight, and a deep commitment to public empowerment.

Through teaching, writing, and speaking, Dr. Poe helps individuals, families, and organizations understand emerging technologies, recognize digital threats, and build the skills needed to live freer and safer in a connected world.

Technology should serve people. Knowledge should be within reach. A safer tomorrow is possible — and we build it together.

— *Rev. Dr. Gerald F. Poe, Jr.*



HOW TO USE THIS GUIDE

SIMPLE STEPS. REAL PROTECTION. A BRIGHTER TOMORROW.

PEOPLE
TECHNOLOGY
A SAFER
TOMORROW

This guide gives you practical knowledge to recognize threats, make safer choices, and take control of your digital life. You don't need to be a tech expert — just a willing learner. Use these five steps anytime you face a suspicious message, call, email, or website.

PAUSE

Take a moment. Don't rush.

Scammers want you to react quickly. Stop, breathe, and think before you click, reply, or share.

VERIFY

Check that it's real.

Confirm the person, organization, or website through a trusted, official source — not the contact info in the message.

PROTECT

Guard your information.

Keep your personal data, passwords, and financial details private. Use strong passwords and enable multi-factor authentication.

REPORT

Speak up.

Report scams and suspicious activity to the proper authorities, your organization, or the platform where it occurred. Your report can help protect others.

RECOVER

Take action and move forward.

If you've been targeted, take steps to secure your accounts, monitor for further activity, and get support. Mistakes happen — recovery is possible.

KNOW MORE • STAY SAFER • LIVE FREER

PoeTech Principles

"Never surrender trust simply because a screen knows your name."

"If a voice asks for money, verify the person."

"Your password protects an account. Your judgment protects your life."

SCRIPTURE FOR THE JOURNEY

"Be wise as serpents and innocent as doves."

MATTHEW 10:16

AWARENESS
PREVENTION
PROTECTION
EMPOWERMENT

Cybersecurity 101

SIMPLE HABITS. STRONGER PROTECTION.
A SAFER TOMORROW.

PEOPLE
TECHNOLOGY
A SAFER
TOMORROW

Cybersecurity means keeping your devices, accounts, and personal information safe from people who want to steal, scam, or cause harm. It's not just about experts and complex tools. It's about everyday choices.



DEVICE
Your phone, laptop, or tablet. Keep it locked, updated, and free from unknown apps.



ACCOUNT
Your login to a service (like email, banking, or social media). Secure your accounts and use strong, unique credentials.



DATA
Your personal information, photos, messages, and files. Treat your data like something valuable, because it is.



PASSWORD MANAGER
A tool that creates and stores strong, unique passwords for you. You only need to remember one master password.



PASSKEY
A newer, safer way to sign in using your device (like a fingerprint, face, or PIN) instead of a traditional password.



MFA (Multi-Factor Authentication)
Adds an extra step (like a code or fingerprint) when you sign in. Even if someone gets your password, they still can't easily get in.



ENCRYPTION
Scrambles your data so only the right people can read it. It protects your messages, files, and online activity.



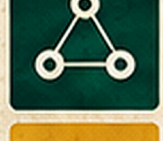
UPDATES
Fix security problems and keep your device and apps safer. Turn on automatic updates when possible.



BACKUPS
Keep copies of your important files (in the cloud or on an external drive) so you can recover them if something goes wrong (like a hack or device loss).



ATTACK SURFACE
All the ways someone could try to reach you, like your devices, accounts, apps, and online profiles. Keep it small by removing what you don't use.



WHY MOST ATTACKS TARGET PEOPLE BEFORE MACHINES
It's usually easier to trick a person than to break a strong system. Attackers use emotions like fear, urgency, and curiosity to get you to click, share, or act. That's why awareness is so powerful.



KNOW MORE
STAY SAFER
LIVE FREER



The First Firewall

Human judgment is still the first firewall.

AI 101 and Superintelligence 101

BIGGER POSSIBILITIES. REAL RISKS.
A SAFER TOMORROW.

KNOW MORE
STAY SAFER
LIVE FREER

What is AI?

Artificial Intelligence (AI) is software that can recognize patterns in large amounts of data and use those patterns to generate text, images, audio, and predictions. Examples include chat assistants, image generators, voice tools, and recommendation systems.

Common Risks

AI can be misused by criminals to:

- Create deepfake voices that sound like real people.
- Generate fake images or videos that look real.
- Run scam chatbots that trick you into sharing information or sending money.
- Launch automated phishing messages at massive scale, making scams more convincing and harder to spot.

Defensive Uses

AI can also help us stay safer by:

- Summarizing security alerts and explaining risks.
- Spotting suspicious language in emails and messages.
- Comparing messages to detect inconsistencies or scams.
- Generating stronger, safer passwords.
- Teaching security basics in simple, clear language.

What is Superintelligence?

Superintelligence refers to future AI systems that may outperform humans across many complex thinking tasks, such as reasoning, planning, problem-solving, and creativity. It's not here yet, but experts believe it could arrive in the future and bring both extraordinary benefits and serious risks.

What Should Ordinary People Do Now?

You don't need to be an expert. Focus on:

- Building AI literacy (understand the basics).
- Verifying information (don't blindly trust what you see or hear).
- Using AI safely and responsibly.
- Staying curious and informed as the technology evolves.

> "If an image demands action, verify the source."



HOW SCAMMERS AND HACKERS REALLY ATTACK

DIFFERENT TACTICS
SAME GOAL
YOUR DATA
YOUR MONEY
YOUR TRUST

Scammers and hackers use a variety of tricks to manipulate, confuse, and deceive. Here are the most common methods you need to know—and how they work.



PHISHING

Fake emails that look legitimate, designed to steal your information or get you to click a malicious link.



SMISHING

Fraudulent text messages (SMS) that trick you into revealing personal data or clicking a bad link.



VISHING

Phone calls from fraudsters who pose as banks, government agencies, or tech support to steal your information.



MALWARE

Malicious software that infects your device, steals data, spies on you, or gives attackers remote control.



FAKE TECH SUPPORT

Scammers pose as legitimate tech support, claiming your device has a problem, then trick you into giving them access or making a payment.



QR CODE SCAMS

Fake QR codes that send you to malicious websites or download malware.



CREDENTIAL STUFFING

Attackers use stolen usernames and passwords from past breaches to break into your other accounts.



SIM SWAPPING

Fraudsters trick your mobile carrier into transferring your phone number to a new SIM card, giving them access to your texts, calls, and accounts.



ROGUE WI-FI

Fake public Wi-Fi networks that look legitimate, but allow attackers to intercept your data.



MALICIOUS LINKS IN PORN OR SHOCK-CONTENT

Links hidden in adult sites, fake videos, or sensational headlines that install malware or steal your information.



THE PSYCHOLOGY BEHIND IT

Scammers exploit human emotions. The most common triggers are:

URGENCY "Act now or lose it!"

FEAR "Something bad will happen!"

GREED "Easy money! Big rewards!"

ROMANCE "They care about you!"

CURIOSITY "You have to see this!"

SAME EMOTIONS. DIFFERENT SCAMS. ALWAYS BE SKEPTICAL.

RECOGNIZE
QUESTION
VERIFY
WALK AWAY
STAY SAFER

RED FLAGS AND WHEN TO WALK AWAY

When something feels off, it probably is. Here are the biggest warning signs that you're being targeted—and when to stop and walk away.



Requests for Codes

Anyone who asks for a one-time code, verification code, or password is a red flag.



Payment by Gift Card or Cryptocurrency

Scammers often demand payment with gift cards, crypto, or other hard-to-trace methods.



Caller ID You Cannot Verify

Caller ID can be spoofed. If you cannot independently verify the caller, do not trust the call.



Pressure to Act Now

If they say "act now," "limited time," or "you'll lose access," it's a tactic to stop you from thinking.



Unknown Attachments

Do not open attachments or download files from people you don't know or weren't expecting.



Password Reset You Did Not Request

If you get a password reset message you didn't ask for, it could be an attempt to take over your account.



Requests for Remote Access

Never allow anyone you do not know to take control of your device (e.g., via AnyDesk, TeamViewer, or similar tools).



Offers Too Good to Be True

Free money, prizes, or unbelievable deals are almost always scams.



HANG UP. CLOSE IT. BLOCK IT.

If you did not initiate the contact, never provide money, passwords, codes, or remote control access. End the conversation, close the message, and block the sender.



> "In cybersecurity, curiosity without caution can become an unlocked door."