Cybersecurity Lunch & Learn

Protecting What Matters Most: Your Identity, Your Finances, Your Peace of Mind

Prepared by Mike Murphy

Your Trusted Partner for Personal & Business Cybersecurity

At **IT GOAT**, we protect people, families, and organizations from the rising threats of identity theft, financial fraud, and digital scams.

We believe cybersecurity should feel:

- **Clear, not confusing**
- **Proactive, not reactive**
- **Personalized, not one-size-fits-all**
- **Human, not automated overseas support**

With a fully USA-based team, industry-leading response times, and a white-glove service approach.

Founder of IT GOAT

Mike has over a decade of experience improving IT and cybersecurity for organizations and protecting them from emerging threats.

- Leads one of the fastest-response cybersecurity teams in the U.S.
- Specializes in helping organizations strengthen cybersecurity and reduce risk.

IT GOAT
Less IT. More Business.

RESOLUTION

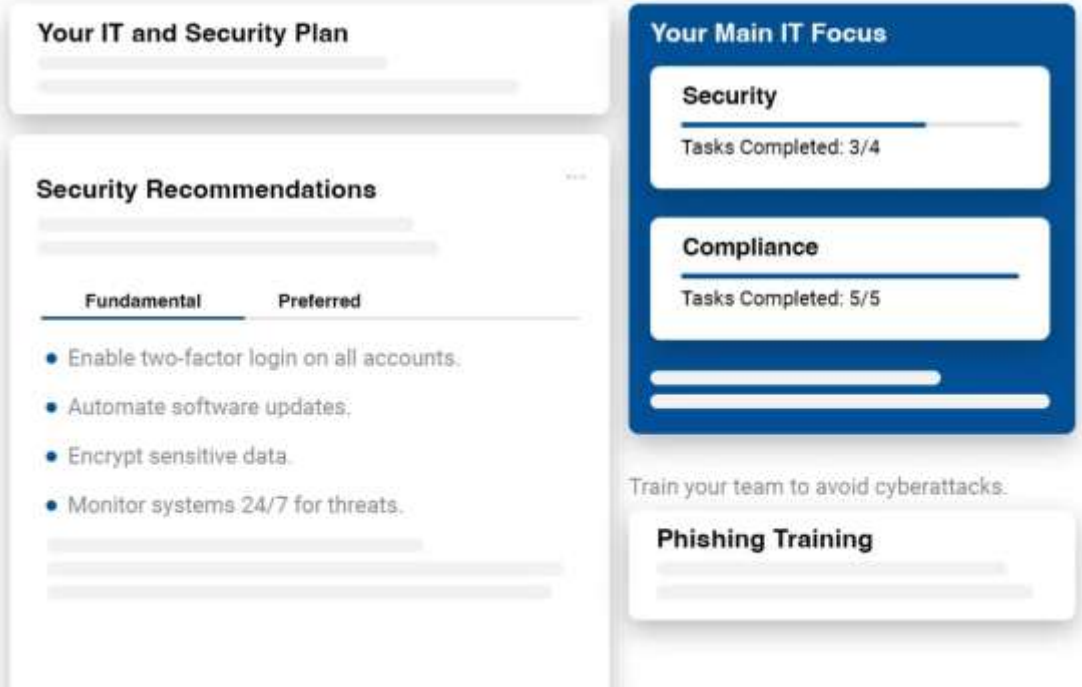
92%

OF TICKETS ARE SOLVED DURING THE FIRST TOUCH POINT

COMPLIANCES

25+

COMPLIANCE STANDARDS OUR TEAM WORKS WITH



Rising Frequency of Attacks

Between 2023 and 2025, the percentage reporting **targeted attacks on executives increased from 43% to 51%.**

Of those impacted in 2025, **22% had experienced 7 to 10 cyber attacks**, an increase of 32% over 2023.

Concern over potential attacks in the future remains consistently high at 62%.

Cybercrime Has Become Personal — And It's Targeting Older Adults

- Scammers assume retirees are easier targets
- Emails and texts now look completely real

IT GOAT
Less IT. More Business.

Top 8 Common Scams

1. Toll Road / Unpaid Fee Text Message Scam

Claim: “You have an unpaid toll fee of $3.12 — pay now to avoid penalties.”

How to Avoid It: Never click payment links from texts; go directly to the official toll website.

2. Fake Package Delivery Notice

Claim: “Your package couldn’t be delivered — update your address here.”

How to Avoid It: Check your delivery app (Amazon, UPS, USPS) instead of clicking links.

3. Bank or Credit Card Fraud Text (Fake)

Claim: “Your debit card is locked due to suspicious activity — verify here.”

How to Avoid It: Call the number on the back of your card, not the message sender.

4. Tech Support Pop-Up Scam

Claim: “Warning! Your computer is infected. Call Microsoft immediately.”

How to Avoid It: Close the browser and never call numbers from pop-up warnings.

Top 8 Common Scams

5. Family Emergency / Grandparent Scam

Claim: “Grandma, I’m in trouble — I need money right now, please don’t tell anyone.”

How to Avoid It: Hang up and call the real family member to verify.

6. Fake Online Stores & Flash Sales

Claim: “Today only! 80% off — limited stock remaining!”

How to Avoid It: Only shop on trusted websites and check reviews before purchasing.

7. IRS / Social Security Impersonation

Claim: “Your SSN has been suspended due to suspicious activity — immediate action required.”

How to Avoid It: Remember: federal agencies never call or text demanding money.

8. Zelle / Venmo “Transfer Reversal” Scam

Claim: “You sent money by mistake — we need to reverse the transaction.”

How to Avoid It: Never send money to “correct” an error; contact your bank directly.

Threat Actor Tactics & Techniques

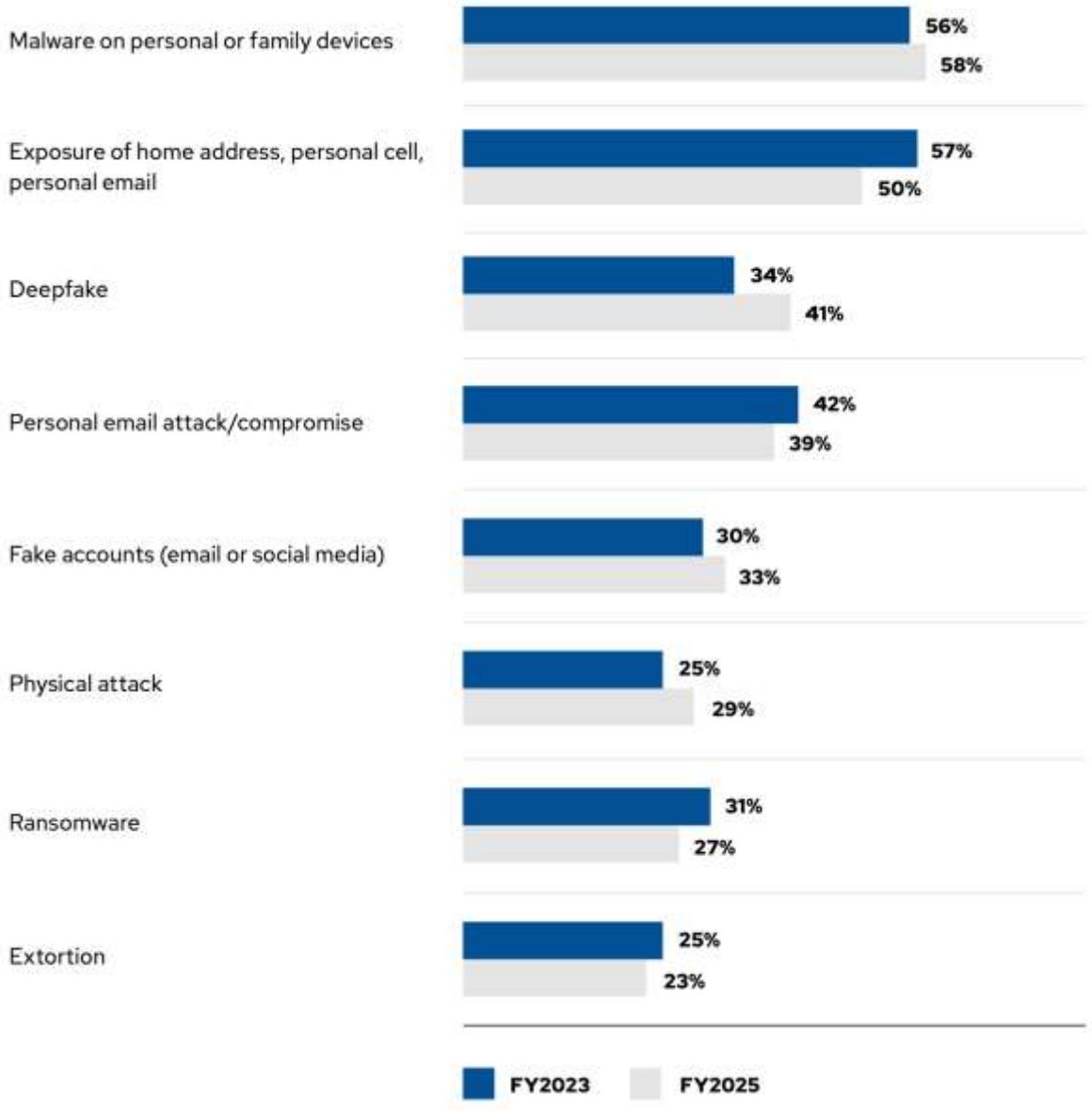
What types of attacks did you experience?

One wrong click can expose your identity and sensitive data that leads to massive financial burdens and headaches.

How do they get your information?

- Impersonate family members
- Password theft / dark web leaks
- Compromised home Wi-Fi
- Fake “support” calls
- Phishing emails and texts
- Fake messages on Facebook & social media

Threats are increasing — but preventing them is possible.



Your First Line of Defense

1. DON'T CLICK LINKS - If you didn't expect the message, delete it — even if it looks real.

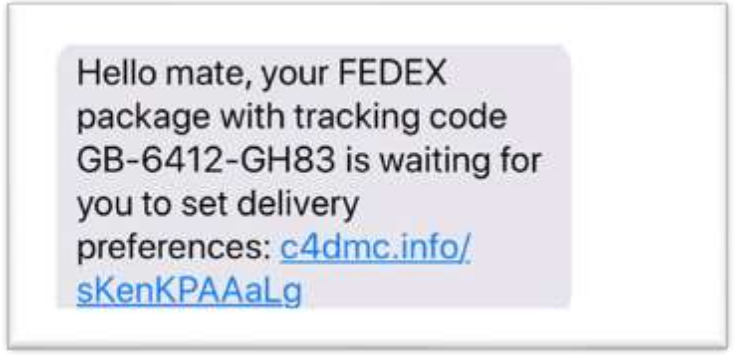
2. DON'T PAY - Never send money, gift cards, or Zelle payments.

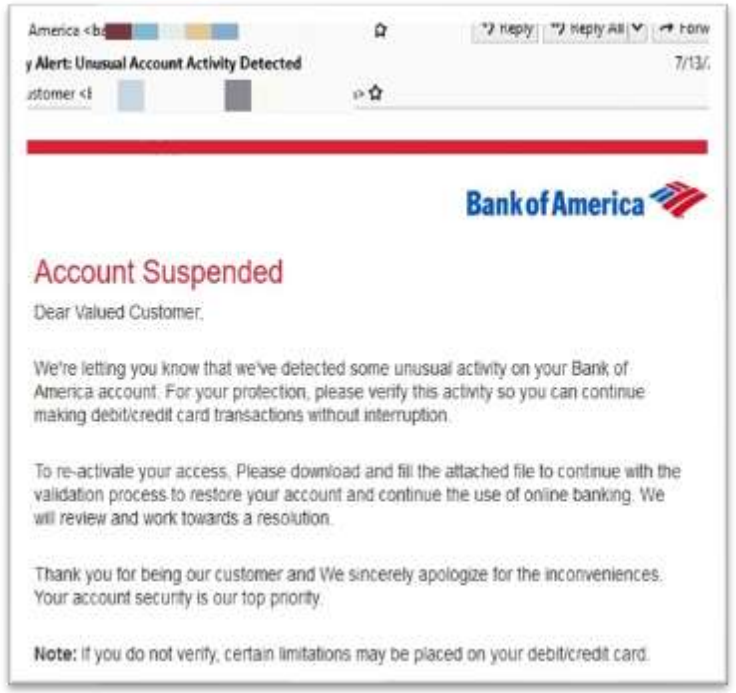
3. DON'T SHARE PERSONAL INFO - No one legitimate will ask for your SSN, passwords, or banking info by phone, text, or email.

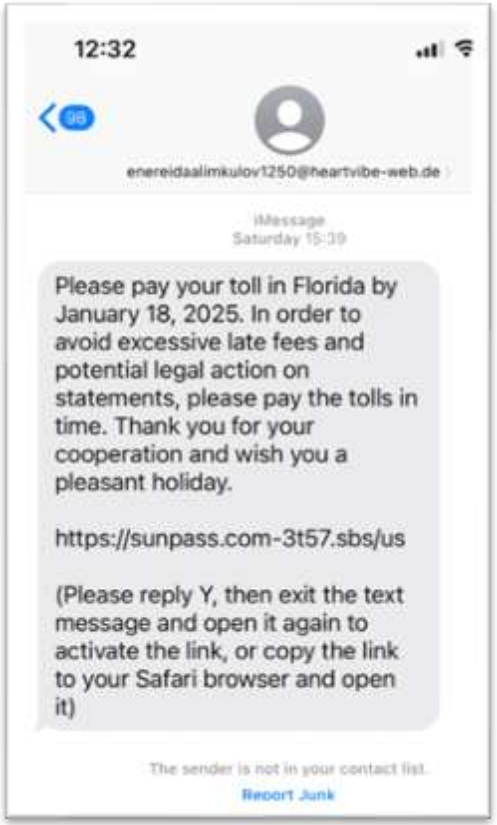
4. DON'T TRUST CALLER ID - Scammers can fake any number — even your bank or the police.

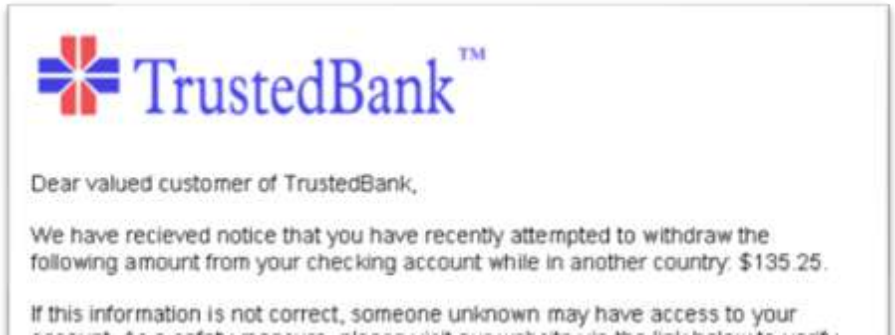
5. DO VERIFY FIRST - Hang up and call the official number printed on your card or statement.

6. DO SLOW DOWN - Scammers create urgency; taking 10 seconds to pause can prevent a costly mistake.









How to be Smarter

1. Maximize Your Facebook Privacy Settings
Set your Facebook privacy to the highest level, avoid sharing photos publicly, and never accept friend requests from people you don't know — **scammers use your profile details to build convincing attacks.**

2. Be Careful Posting Personal Details Online
Avoid posting names of pets, family members, birthdays, or anything you use for security questions — **scammers use this information for social engineering and account recovery scams.**

3. Secure Your Home Wi-Fi Network
Use a strong, unique Wi-Fi password; if it's easy to guess,
criminals can access your smart cameras, doorbells, and personal devices inside your home.

4. Use Multi-Factor Authentication (MFA) — But Never Share Codes
Always enable MFA, but remember: **no legitimate company will ever ask for your MFA code** — if you didn't request it, you should never receive it.

5. Set Up Bank Withdrawal & Transaction Alerts
Turn on mobile and email alerts for every withdrawal or purchase —
you'll catch fraud instantly before it becomes a larger issue.

The Part No One Talks About...

Even if you do everything right, you're still exposed to risks you can't see.

- Your passwords may already be on the **dark web**
- Your information might be circulating on **data broker sites**
- Your home network could have **hidden vulnerabilities**

AI can now fake voices, photos, and even family members

And most importantly...

Most people don't know the moment they've been hacked.

- Your devices won't warn you.
- Your bank won't warn you.
- Your email won't warn you.
- No one knows — until it's too late.

The most realistic #Deepfake you've seen

It’s Too Much to Manage Alone

This is a LOT for one person to keep up with.

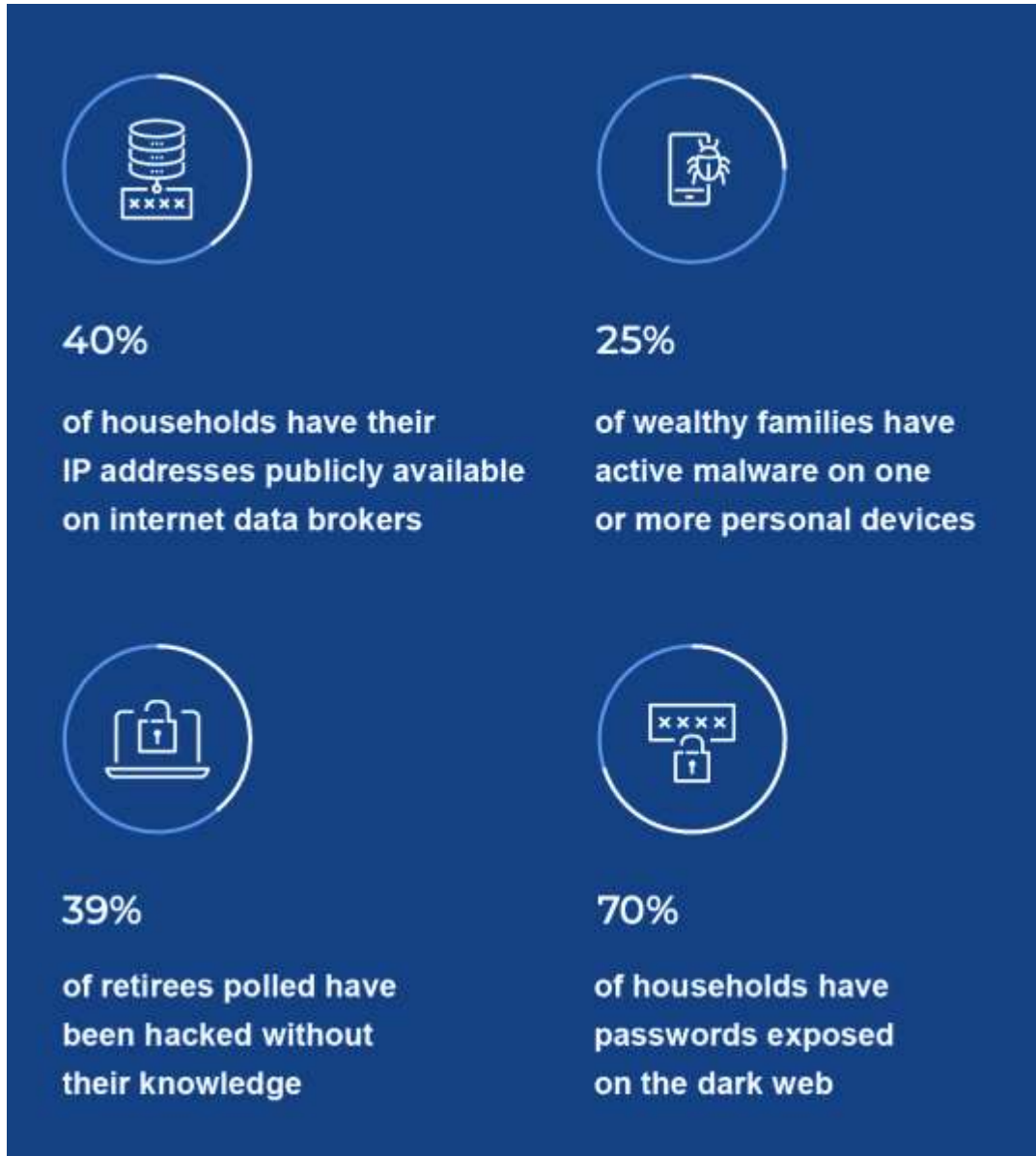
- Scams evolve every month
- Attacks are becoming personalized
- Criminals work 24/7
- There’s no instruction manual
- And most people feel alone when something goes wrong

That’s why so many people, especially retirees — tell us the same thing:

“I want to be safe… I just need someone to guide me.”

“I just wish there was someone I could trust to tell me what’s real and what’s not.”

“I don’t want to bother my kids… but I don’t want to get tricked either.”



NEXUS ONE FINANCIAL ADVISORS

Protect Your Digital Life

IT GOAT Less IT. More Business.

IT GOAT has partnered with Nexus One Financial Advisors to help you stay safe, secure, and supported — every day.

NEXUS ONE FINANCIAL ADVISORS

White-Glove Protection Suite

IT GOAT Less IT. More Business.

Our Platform

A **holistic solution** combining software and services for both cybersecurity & privacy

Protect Their Privacy

- Data Broker Removal
- Dark Web
- Device Hardening
- VPN

Protect Their Devices

- Endpoint
- Deception / Honeypot
- Malicious Calendar

Protect Their Home

- Weekly Vulnerability Tests
- IoT / Cameras
- Network Review

Protect Their Peace of Mind

- Incident Response
- CISO Insights
- Education & Training

NEXUS ONE FINANCIAL ADVISORS

Security Made Simple

IT GOAT Less IT. More Business.

Concierge-Level Protection Platform

Protect Your Digital Lives – anywhere, anytime

Mobile and desktop experiences

for easy access, wherever you are

Intuitive visualizations

show your risk at a glance

24/7/365 monitoring

by the BlackCloak SOC

Monitor

your personal, home, and family devices

Real-time updates and reporting

show you exactly where your security stands at any moment

Education portal

provides you with up-to-date security tips and industry news

NEXUS ONE FINANCIAL ADVISORS

Subscription Plans and Pricing

IT GOAT Less IT. More Business.

	Professional	Executive	Principal
	$5,500/per year for the first adult	$7,250/per year for the first adult	$8,750/per year for the first adult

Additional family members may be added to any plan for $1,250/adult. Dependents under 18 are free.

Essential Cybersecurity & Privacy	• Incident Response
	• Concierge Assistance (M-F)
	• Home Network Scan (Weekly – 1 Home)
	• Device Protection & Monitoring
	  - Mobile Devices
	  - Computers
	• Deep/Dark Web Scan (Daily)
	• VPN
		• Incident Response
		• Concierge Assistance (M-F)
		• Home Network Scan (Weekly – 2 Homes)
		• Device Protection & Monitoring
		  - Mobile Devices
		  - Computers
		• Deep/Dark Web Scan (Daily)
		• VPN
			• Incident Response
			• Concierge Assistance (7 Days a Week)
			• Home Network Scan (Weekly – Unlimited)
			• Device Protection & Monitoring
			  - Mobile Devices
			  - Computers
			• Deep/Dark Web Scan (Daily)
			• VPN

Enhanced Privacy	• Personal Information Removal from Internet Data Brokers	• Personal Information Removal from Internet Data Brokers • Device Privacy Hardening • Credit Monitoring* • Identity Theft Protection* • Up to $1 Million Identity Theft Insurance**	• Personal Information Removal from Internet Data Brokers • Device Privacy Hardening • Credit Monitoring* • Identity Theft Protection* • Up to $1 Million Identity Theft Insurance**
Enhanced Cybersecurity		• Deception • Dual-Factor Authentication Training (Email, Bank, Social Media)	• Deception • Dual-Factor Authentication Training (Email, Bank, Social Media) • Password Safe Training • Social Media Impersonation Removal (On Demand)

Corporate agreements include anonymized, aggregate reporting on a quarterly basis and include a $500 onboarding fee per executive.

Additional adults and dependent children must be part of the same household— i.e. they reside together or are an immediate family member.

IT GOAT

Mike Murphy
President

469-444-9004
mmurphy@itgoat.com
www.itgoat.com

11,000+ Industry Certifications

25+ Years Of Cybersecurity

1,700+ Certified Technical Experts

IT GOAT
Less IT More Business.

Download Your Copy