



Bosch Insurance Group
Protecting your future today

DON'T GET SCAMMED

A Practical Guide to Protecting Yourself & Your Family

Presented by

BOSCH INSURANCE GROUP

The goal of this guide

You do not need to memorize every new scam. Learn the patterns scammers use, slow the situation down, verify independently, and build layers of protection around your identity and digital life.

STOP • HANG UP • VERIFY

The Story Changes. The Tactics Usually Don't.

Scammers have better tools than they used to. They can disguise caller ID, send convincing texts and emails, impersonate familiar organizations, and use artificial intelligence to imitate voices. Something that looks or sounds legitimate may still be fake.

The good news is that most scams still depend on a small number of human reactions. If you learn to recognize those patterns, you can make yourself a much harder target.

One rule worth remembering

When an unexpected contact creates strong emotion and demands immediate action involving money, personal information, or access to a device, stop the conversation and verify it independently.

Four ingredients show up again and again

- Trust - the person claims to be someone you recognize or respect.
- Emotion - fear, excitement, concern, embarrassment, or confusion takes over.
- Urgency - you are told to act now, stay on the line, or keep the situation secret.
- The ask - money, account information, passwords, verification codes, identity data, or computer access.

1. Slow Down: Your Best Defense

Scammers benefit when you react before you think. A legitimate organization can usually give you enough time to verify what is happening.

Use the three-step rule

STOP

Do not send money, provide sensitive information, click a link, or install software.

HANG UP

End the incoming call or conversation. You do not owe an unexpected caller an explanation.

VERIFY

Find the organization's contact information yourself and make a new call. For family emergencies, contact the family member or another relative directly.

Never rely only on a phone number, link, or contact method supplied by the person you are trying to verify.

2. Caller ID, Texts and Emails Can Be Deceptive

A familiar company name or local number on your screen is not proof of identity. Criminals can manipulate how calls appear and can create messages that look remarkably similar to legitimate communications.

Safer habits

- For a bank or credit-card concern, call the number printed on your card or statement.
- For a government concern, find the agency's official contact information independently.
- Do not sign in to an account through an unexpected text or email link.
- Do not provide a one-time verification code to someone who contacted you.
- Be skeptical when a caller objects to you hanging up and calling back.

Simple rule

Trust the contact you initiate more than the contact that unexpectedly initiates with you.

3. Common Scam Patterns

Tech-support scams

A pop-up, phone call, or message claims your computer has been infected or compromised. The person offers to diagnose the problem and asks you to install remote-access software.

- Do not give an unsolicited caller remote access.
- Do not call numbers displayed in alarming pop-ups.
- If concerned, shut the device down and contact a trusted technician independently.

Bank and credit-card impostors

The message says suspicious activity has been detected and asks you to verify information, move money, or provide a security code.

- End the conversation.
- Call your financial institution directly using a trusted number.
- Never move money to a 'safe' account because an incoming caller tells you to.

Government impostors

The caller claims to represent Social Security, Medicare, the IRS, a court, or law enforcement and uses authority or threats to force quick action.

- Do not let a badge number or official-sounding title rush you.
- Independently contact the agency.
- Treat unusual payment demands as a major warning sign.

4. Family Emergency & AI Voice Scams

A call involving a child, grandchild, spouse, or other loved one can bypass normal skepticism because the emotional stakes feel immediate. AI voice tools make a familiar-sounding voice less reliable as proof of identity.

Create a family verification plan now

- Choose a private family safe word or phrase that is not posted online.
- If someone claims a relative is in trouble, hang up and call that relative directly.
- If you cannot reach them, call another family member who can verify the story.
- Be suspicious of requests for secrecy, especially 'don't tell Mom,' 'don't call anyone,' or 'stay on the phone.'
- Never let embarrassment stop you from asking someone else for a second opinion.

Family rule

No large or unusual financial decision gets made because of an unexpected call, text, or email without first verifying it with someone else.

5. Medicare, Prize, Utility & Investment Scams

Medicare-related scams

Unsolicited callers may offer equipment, tests, services, or benefits while asking you to confirm personal or Medicare information. Knowing your name, doctor, address, or other details does not prove the caller is legitimate.

Sweepstakes and prizes

A large prize followed by a request for taxes, fees, gift cards, or advance payment is a major warning sign. Ask yourself whether you even entered the contest.

Utilities and service providers

Threats of immediate shutoff or promises of unusually large savings can create urgency. End the call and contact the company using information from a bill or other trusted source.

Investments and cryptocurrency

Be cautious of unusually high returns, little or no risk, exclusive opportunities, or pressure to act before you can investigate. A professional-looking website or account balance on a screen does not prove the investment is real.

6. Why Smart People Can Still Be Fooled

Fraud is not simply an intelligence problem. Timing and emotional state matter. People can be easier to manipulate when they are tired, distracted, grieving, under financial pressure, caring for someone, dealing with major life changes, or excited about an unexpected opportunity.

That is why the best response to a high-pressure situation is often not to analyze it faster - it is to interrupt it.

Give yourself permission to stop

You can hang up. You can wait. You can call someone. You can verify. You can decide tomorrow.

The two-minute scam test

- Why does this have to happen right now?
- Can I independently confirm who this person is?
- Why do they need this money or information?
- Who can I talk to before I act?
- Would I still make this decision if I had 24 hours to think about it?

7. Ten Warning Signs Worth Remembering

1. Unexpected contact involving money or sensitive information.
2. Pressure to act immediately.
3. Instructions not to hang up.
4. A request to keep the situation secret.
5. Threats of arrest, account closure, shutoff, or another serious consequence.
6. An unusual method of payment.
7. A request for remote access to your computer or phone.
8. A request for passwords or verification codes.
9. Promises of unusually large rewards or returns with little risk.
10. Anger, intimidation, or resistance when you say you want to verify the story.

Remember

One warning sign does not automatically prove fraud. Several warning signs appearing together should cause you to stop and independently verify the situation.

8. Awareness Is Important - But It Is Only One Layer

Recognizing a scam can help you stop an attack that reaches you. But awareness cannot tell you about every problem happening outside your view. Personal information may already be circulating online, an account may be targeted, or identity misuse may begin without an obvious phone call or text.

Think in four layers

1. AWARENESS

Recognize manipulation, suspicious contacts, and common scam patterns.

2. PREVENTION

Reduce unnecessary exposure, use stronger account security, and protect devices.

3. MONITORING

Watch for signs that identity or financial information may be misused.

4. RECOVERY

Know where to turn for help if identity theft or another digital problem occurs.

No product or service can guarantee that fraud, identity theft, or cybercrime will never happen. The objective is to reduce exposure, identify potential problems sooner, and have a response plan.

9. An Optional Resource: iDefend

For readers who want protection beyond education alone, Bosch Insurance Group makes iDefend available as an optional resource.

According to iDefend's current service terms, its offerings can include identity-theft monitoring and alerts involving areas such as credit, account takeover, Social Security benefits, medical identity, tax-return fraud, criminal records, financial accounts, and dark-web activity. Features and monitoring vary by plan, and some services require account setup and activation.

The important distinction is that a service like this is not a substitute for good judgment. It is another layer that can complement the habits in this guide.

The goal is not fear. It is preparedness.

Learn the warning signs. Reduce your exposure. Add monitoring where appropriate. Have help available if something happens.



SCAN TO LEARN MORE ABOUT IDEFEND

https://www.idealhome.com/lp/protection-ia/?p_id=BIG

Affiliate disclosure: Bosch Insurance Group may receive compensation if you enroll in iDefend through this referral link.

iDefend does not guarantee protection against all threats or reimbursement of actual financial losses. Services and monitoring vary by plan.

10. Scam Protection Checklist

- ☐ Use unique, strong passwords for important accounts.
- ☐ Turn on multi-factor authentication where available.
- ☐ Keep phones, computers, browsers, and security software updated.
- ☐ Do not give remote computer access to an unsolicited caller.
- ☐ Never share one-time verification codes with someone who contacted you.
- ☐ Verify financial or government concerns using contact information you find independently.
- ☐ Create a family safe word for emergency calls.
- ☐ Discuss large or unusual money requests with someone you trust before acting.
- ☐ Review financial accounts and statements for unfamiliar activity.
- ☐ Be cautious about how much personal information you make public online.
- ☐ Consider monitoring and identity-recovery services if they fit your needs.
- ☐ Save this rule: STOP. HANG UP. VERIFY.

If you think you have been scammed

Contact the affected bank, credit-card issuer, service provider, or other institution promptly. Change compromised passwords, secure affected accounts, and report the incident to the appropriate authorities or consumer-protection agency.

A Final Thought

Technology will keep changing, and scammers will keep changing their stories. Trying to memorize every new fraud scheme is nearly impossible.

Instead, remember the pattern:

UNEXPECTED CONTACT
TRUST
EMOTION
URGENCY
A REQUEST FOR MONEY, INFORMATION OR ACCESS

When those pieces begin coming together, you do not need to outsmart the person on the other end. End the interaction and verify what is happening independently.

STOP. HANG UP. VERIFY.

Bosch Insurance Group

Consumer education focused on helping individuals and families make informed decisions.

Educational disclaimer: This guide is for general educational purposes and is not legal, financial, cybersecurity, or law-enforcement advice. Scam methods and digital threats change frequently. Product descriptions are general and should be confirmed against current service terms before enrollment.