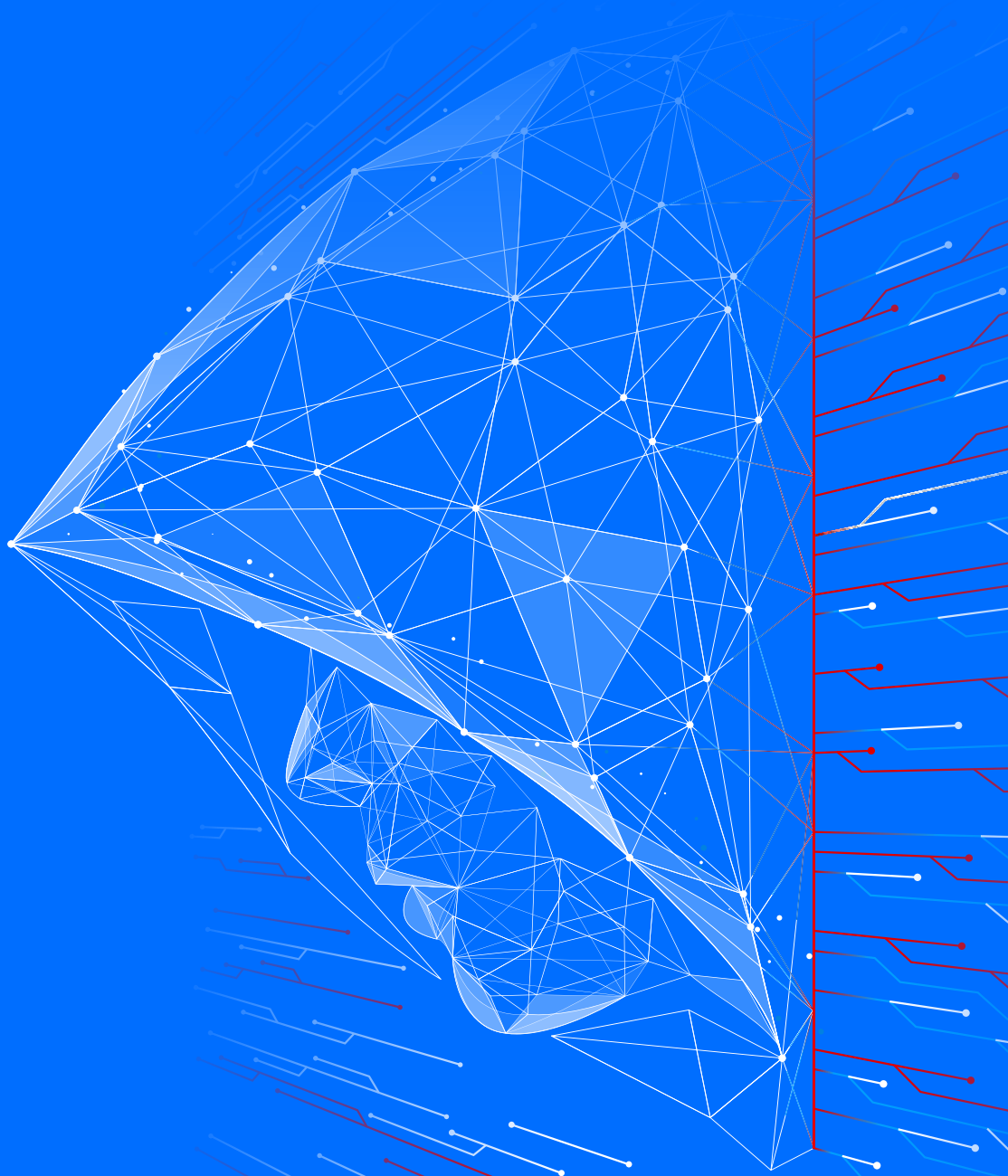
Bitdefender

WHITEPAPER

Why Smart People Fall for Scams and How to Protect Yourself

A practical guide to the most common scams targeting families today



Scams are no longer rare events that happen to "other people."

More than half of adults worldwide say they have experienced a scam, and nearly a quarter lost money in the past year alone*. When it happens, it often unfolds quickly, in roughly two-thirds of cases, the situation escalates within a single day of the first contact.

If you use a phone, email, or social media, you are already in the space where scams happen. Attempts arrive through everyday channels: phone calls (53%), text messages (51%), and email (47%), as well as familiar apps like WhatsApp (53%), Facebook (41%), Gmail (38%), and Instagram (27%).

This guide helps you understand why smart people fall for scams, and how to protect yourself and your family.

Not long ago, red flags were easier to spot: poor grammar, strange email addresses, clumsy websites. Today, scammers use AI to write natural-sounding messages, clone voices, and create convincing deepfake videos. Fake websites can mirror legitimate ones almost perfectly, and researchers have even found that AI-generated faces can appear more trustworthy than real ones*.

Many scams are personalized using information about you gathered from social media, referencing real names, workplaces, or recent events. They create urgency, exploit authority, and often reach you when you are stressed or distracted.

That is why falling for a scam is not a sign of carelessness. In the right moment, under the right pressure, even thoughtful and intelligent people can be pushed to act quickly.

How Scams Reach Every Generation in Your Family

Scammers pay attention to age, habits, routines, and the platforms each person uses. In the same household, a child might be approached inside a game, a teenager through social media, and a parent through a banking message.

The categories below help us understand patterns, but they are not rules, almost any type of scam can be reshaped to target anyone.

Scams Targeting Children

Children trust easily, especially in environments that feel familiar and fun.

Gaming-related scams

Inside games like Roblox or Minecraft, scammers may pose as other players and slowly build a connection. They talk, play together, and gain trust before offering something tempting — rare skins, secret levels, exclusive items, or "free Robux." This can quickly shift into requests for login details or help "just confirming something," sometimes leading to charges on a parent's credit card.

In-app purchases and fake rewards

Pop-ups and messages can promise free coins, V-Bucks, special upgrades, or bonus rewards. To unlock them, children are asked to click a link or enter account information. In other cases, repeated in-app purchases are encouraged through platforms linked to Apple Pay or Google Play.

Impersonation of favorite creators or characters

Scammers impersonate creators like MrBeast, Dhar Mann, or well-known gaming influencers, announcing fake giveaways or "exclusive" contests. A direct message offering a prize can feel exciting and real. In that excitement, children may share personal details, verification codes, or payment information without realizing the risk.

Social engineering through game chats and messaging apps

Many games include chat functions, and conversations often move to platforms such as Discord or WhatsApp. Once there, the interaction becomes more private and harder for parents to notice. Scammers use that space to request downloads, encourage screen sharing, or ask for personal information.

Requests to share personal details or account access

Children may be asked to share passwords, verification codes, or access "just for a minute." What feels like helping a new online friend can quickly turn into a stolen account, lost progress in a favorite game, or unexpected charges.

Scams Targeting Teenagers

They are exploring identity, opportunity, and independence. Scammers exploit that curiosity and ambition, knowing that the desire to grow up faster can sometimes outpace experience.

Sextortion and blackmail

A teen may receive a friendly message on Instagram, Snapchat, or Discord. The conversation feels normal at first, sometimes even flattering. It turns flirtatious, photos are exchanged, and then the tone shifts. The scammer threatens to send the images to friends, classmates, or family unless money is paid immediately.

Fake job, scholarship, or influencer opportunities

Teens looking for part-time work or brand collaborations may receive offers that appear professional. A "recruiter" asks for an upfront fee, identity documents, or bank details. Fake scholarship programs may request application payments. Influencer scams promise sponsorship deals in exchange for buying products first.

"Easy money" schemes

On TikTok, Instagram, or Telegram, trading groups, crypto investments, or "secret" financial communities promise fast profits. Once funds are transferred, the group disappears — or asks for more.

Online shopping scams

Limited-edition sneakers, gaming consoles, concert tickets, or trending fashion items are advertised at attractive prices. Fake websites and social media ads mimic legitimate brands. Once the payment goes through, the scammer disappears, and the product never arrives.

Health and beauty scams

"Miracle" supplements, skincare products, weight-loss programs, or fitness plans promoted by fake influencers target teens who already feel pressure to look a certain way. Some of these schemes lock users into subscriptions. Others collect personal information without delivering anything at all.

Scams Targeting Parents and Working Adults

For adults, scams often blend into ordinary tasks. Scammers target them while managing finances, shopping online, applying for jobs, or paying bills.

"Family emergency" impersonation scam

A parent receives a late-night message: "Mom, I broke my phone. This is my new number." Or a call from someone claiming their child has been in an accident and urgently needs money for medical bills or legal fees. Parents are pushed to act immediately, often told not to involve anyone else.

Bank or delivery impersonation messages

You might receive a text claiming there is suspicious activity on your account and urging you to confirm a transaction immediately, or an email stating that a package cannot be delivered unless a small fee is paid. The message looks routine and the timing feels

plausible, but clicking the link leads to a fake login page created to capture passwords or verification codes.

Fake online stores and marketplace scams

A seller on a marketplace may suggest completing payment outside the platform “to avoid fees,” or a social media ad may promote a heavily discounted product that seems like a good deal. The process feels quick and convenient — until the item never arrives or turns out to be counterfeit.

Crypto, investment, or “side income” opportunities

Adults hoping to grow savings or supplement income may be approached on LinkedIn, WhatsApp, or Telegram with invitations to join trading groups, crypto investments, or “guaranteed return” programs. Professional dashboards and polished testimonials build credibility before larger deposits are requested.

Job scams

A recruiter advertises a remote position with attractive pay and flexible hours. Applicants are asked to pay onboarding fees, purchase equipment, or provide personal documents for verification. In some cases, victims are unknowingly drawn into transferring funds as part of a larger fraud scheme.

Invoice or payment redirection fraud

For small business owners, invoice or payment redirection fraud is especially damaging. An email appears to come from a trusted supplier, contractor, or colleague announcing updated bank details. The invoice itself may be legitimate — only the account number has been changed. By the time the payment is processed, the money has already been redirected.

Scams Targeting Grandparents and Older Family Members

Scammers assume they have savings, a stable income, or may be less familiar with rapidly changing digital tactics. Many attacks are carefully designed to create authority, urgency, or emotional connection.

Impersonation of banks or government agencies

A caller claims to represent a bank, tax authority, social security office, or even law enforcement. There is a supposed problem with an account, unpaid taxes, or suspicious activity that must be resolved immediately.

Romance and companionship scams

Over weeks or months, scammers build emotional relationships, often posing as widowers, military personnel, or professionals working overseas. Conversations feel personal and supportive. Once trust is established, financial requests begin — help with medical bills, travel costs, or temporary financial restrictions. Because the connection feels real, the betrayal can be especially painful.

Pension-related fraud

Older adults may be encouraged to “protect” retirement funds or move savings into higher-return investments. Professional documents, confident language, and references to market trends create credibility. In some cases, victims are told they must act quickly to avoid missing a limited opportunity.

Tech support scams

A caller claims to represent a well-known technology company. The victim is told the device is compromised and must grant remote access so the issue can be fixed. Once access is provided, scammers may install malware, steal personal information, or demand payment for unnecessary repairs.

Warning Signs That Still Matter

Scams today can look polished and professional, so the most important clues are often not in the grammar but in the pressure. Pay attention to how a message makes you feel and what it is pushing you to do.

Here are warning signs that matter:

- **Unusual urgency.** If you are told to act immediately or risk losing money, access, or an opportunity, pause. Legitimate institutions rarely demand instant decisions without giving you space to verify.
- **Pressure to keep it secret.** If someone tells you not to inform your bank, your partner, your colleagues, or anyone else, that request alone should raise concern. Isolation is a common manipulation tactic.
- **Requests to move the conversation off-platform.** Be cautious if the conversation is suddenly moved off the original platform, as it reduces transparency and makes tracing the interaction more difficult.
- **Unusual payment methods.** Requests for gift cards, cryptocurrency, wire transfers, or other non-refundable options are frequently associated with scams because they are hard to reverse once the money is sent.
- **Requests that bypass normal procedures.** Notice when someone asks you to bypass normal procedures or presents unexpected changes, especially if you are pressured to accept them quickly without proper verification.

If something pushes you to act quickly, quietly, or differently than you normally would, pause. That pause is often your strongest protection.

How to Protect Yourself and the People You Love

Scam prevention is about protecting your entire family, the people you love and who rely on you.

Children may not recognize manipulation inside games or social platforms. Teenagers may overestimate their ability to detect risk. Older family members may trust authority too quickly or feel uncomfortable questioning official-sounding requests.

- **Talk openly about scams.**
  Have regular, simple conversations about how scams work and why they succeed. Make it normal to question urgent requests and to ask for a second opinion.
- **Agree on basic family rules.**
  For example: always verify urgent money requests through a second channel, and never share passwords or verification codes — even with someone who sounds familiar.
- **Pause when something feels urgent.**
  Pressure is one of the strongest tools scammers use. Slowing down creates space to think clearly.
- **Verify through official contact details.**
  If someone claims to be your bank, a delivery company, or even a family member, reach out using trusted contact information, not the details provided in the message.
- **Talk to someone you trust before sending money.**
  A quick conversation with a partner, friend, or relative can help you spot patterns you might miss in the moment.
- **Be careful what you share online.**
  Details about your workplace, travel plans, or family members can be used to personalize scams.
- **Use strong, unique passwords and enable two-factor authentication.**
  Even if a password is exposed, an extra layer of protection can prevent access.
- **Protect your phone as carefully as your computer.**
  Many scams now begin through SMS, messaging apps, or mobile browsing.

If Something Feels Wrong — What to Do Next

If you suspect a scam, don't ignore that feeling. Acting quickly can reduce the damage.

- **Stop communication immediately.**
  Do not reply further. Do not click additional links. Even if messages continue, disengage.
- **Do not send more money.**
  Scammers often increase pressure when they sense hesitation. Sending additional funds rarely fixes the situation.
- **Contact your bank or payment provider right away.**
  If you transferred money, shared card details, or approved a transaction, notify them immediately. In some cases, payments can be blocked, reversed, or flagged before further damage occurs.
- **Report the incident.**
  Inform your bank, your telecom provider (if the scam began with a call or SMS), and the platform where it happened. You can also report it to local consumer protection or fraud authorities. Reporting may help protect others and support investigations.
- **Secure your accounts.**
  Change passwords on affected accounts and enable two-factor authentication. If you shared verification codes, act quickly to protect related accounts.
- **Monitor your financial activity.**
  Review bank statements, credit reports, and online accounts in the days and weeks that follow to catch any unusual activity early.

Don't feel ashamed if you were scammed. It's not you, it's scammers who are organized and use every tool available to exploit trust and override your decision-making.

Also, consider getting all the help you can to protect your digital life, devices, data, and money. There are tools and organizations that can support you. The only way to defeat scammers is when people, institutions, and communities work together to stop them.

Sources:

* Global State of Scams 2025 REPORT by GASA.

* https://www.bitdefender.com/en-us/blog/hotforsecurity/ai-faces-more-human-than-human

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-SPP-whitepaper-WSPF-brand344-en_EN
CD-07/30/24 • MD-March 3, 2026 11:13 am