There seems to be more scammers out there than ever before. Part of this is because they can now scan remotely. In the old days scams and cons had to take place in person.

One kind of scam that we're seeing a lot of happens when you're trying to sell something. You put your phone number out there and almost instantly you'll get a text message where they want to send you a code to “prove you are human”. Don’t do it! You will lose your phone contract and find out on the next billing cycle that you just bought the latest iPhone. What is really happening, is they tried to log into your phone provider, when is texting you a code to verify it’s you from another computer. When you give the code to the person, they use it to log into your phone account.

Another scam involves the lonely hearts. They reach out to people and try to build a relationship. This scam falls under the pig butchering style. The way they reach out to you varies. The one I get recently is the wrong number scam. They text and say something like “I'm going to get the ride”. When you tell them “wrong number”. They say “ohh isn't this Lisa?”. From there goes on to some form of “you sound nice, can I buy you a coffee.” They build up a relationship. This will lead to selling you a chance to get rich, or lead the person into a long distance relationship. In both cases you will send them money you will never see again.

A recent scam happens when a phone call comes from your bank (your caller id will be from the bank). The message will tell you about a large transaction that, if you didn’t make it, you need to “contact us immediately” at the number or a link they provide in the message. If you contact them, you will end up losing your money. The bank’s caller id was spoofed, and they message did not come from the bank. If you are worried, just call the bank using the number on the back of the card, or visit the branch and ask them if there is a problem or large transaction.

The Rise of Modern Scams

In today's digital age, scammers have become more prevalent and sophisticated than ever before. The shift from in-person cons to remote scams has significantly expanded their reach and effectiveness.

Common Scam Types

The "Verify You're Human" Scam

When selling items online, be wary of immediate text messages requesting a code to "prove you're human". This is often a ploy to gain access to your phone account. Here's how it works:

1. Scammers attempt to log into your phone provider's account.
2. The provider sends you a verification code.
3. The scammer asks you for this code, claiming it's to verify your humanity.
4. If you provide the code, they gain access to your account.

**Consequences**: You may lose your phone contract and find unexpected charges for new devices on your next bill.

The "Pig Butchering" Scam

This scam targets lonely individuals, building relationships to exploit them financially. A common approach is the "wrong number" tactic:

1. Scammer sends a message meant for someone else.
2. When you respond, they engage in friendly conversation.
3. They gradually build trust and rapport.
4. Eventually, they propose get-rich-quick schemes or long-distance relationships.

**Result**: Victims often send money that they never recover.

The Fake Bank Call Scam

This sophisticated scam involves:

1. A call appearing to come from your bank (using spoofed caller ID).
2. A message about a large, suspicious transaction.
3. Instructions to contact them immediately via a provided number or link.

**Warning**: Contacting the scammers through their provided methods can lead to financial loss.

Protecting Yourself

* Never share verification codes with anyone.
* Be skeptical of unsolicited messages and unexpected relationships.
* Verify bank concerns directly through official channels (e.g., the number on your card or by visiting a branch).

Remember, staying informed and cautious is your best defense against these evolving scams.

More info on scams   
https://www.reddit.com/r/Scams/  
They have about 40 different kinds of scams defined in the ‘about’ section

The ‘more’ on the bank scam

The Evolution of Bank Scams: From Door-to-Door to Digital

Long before the internet era, a sophisticated form of bank fraud known as the "bank examiner scam" preyed on unsuspecting victims, particularly targeting vulnerable individuals such as the elderly. This scam operated as follows:**The In-Person Approach**  
Two well-dressed men, posing as bank officials or law enforcement agents, would visit an elderly person's home. They would claim to be investigating a dishonest bank teller suspected of embezzlement.**The False Narrative**  
The scammers would explain that they needed the victim's help to catch the supposed thief. They would request that the victim withdraw a significant sum of money from their account, which would then be used as "bait" to trap the dishonest employee.**The Deception**  
The fraudsters would assure the victim that the money would be immediately redeposited, claiming this process would help identify the teller who was manipulating accounts.

The Digital Transformation

In the modern era, this scam has undergone a significant transformation:**Online Reach**  
Today's scammers no longer need to physically visit their targets. Instead, they exploit the internet's vast reach to contact potential victims through emails, social media, or fraudulent websites.**Wider Net**  
The digital version of this scam can target a much larger pool of potential victims simultaneously, increasing its efficiency and potential for success.**Varied Tactics**  
While the core deception remains similar, online scammers often employ more diverse and sophisticated tactics, such as phishing emails, fake banking websites, or social engineering techniques.The transition from in-person to online scams highlights the adaptability of fraudsters and underscores the importance of digital literacy and cybersecurity awareness in the modern age.

<div>

<h2>The Evolution of Bank Scams: From Door-to-Door to Digital</h2>

<p>Long before the internet era, a sophisticated form of bank fraud known as the "bank examiner scam" preyed on unsuspecting victims, particularly targeting vulnerable individuals such as the elderly. This scam operated as follows:</p>

<h3>The In-Person Approach</h3>

<p>Two well-dressed men, posing as bank officials or law enforcement agents, would visit an elderly person's home. They would claim to be investigating a dishonest bank teller suspected of embezzlement.</p>

<h3>The False Narrative</h3>

<p>The scammers would explain that they needed the victim's help to catch the supposed thief. They would request that the victim withdraw a significant sum of money from their account, which would then be used as "bait" to trap the dishonest employee.</p>

<h3>The Deception</h3>

<p>The fraudsters would assure the victim that the money would be immediately redeposited, claiming this process would help identify the teller who was manipulating accounts.</p>

<h2>The Digital Transformation</h2>

<p>In the modern era, this scam has undergone a significant transformation:</p>

<h3>Online Reach</h3>

<p>Today's scammers no longer need to physically visit their targets. Instead, they exploit the internet's vast reach to contact potential victims through emails, social media, or fraudulent websites.</p>

<h3>Wider Net</h3>

<p>The digital version of this scam can target a much larger pool of potential victims simultaneously, increasing its efficiency and potential for success.</p>

<h3>Varied Tactics</h3>

<p>While the core deception remains similar, online scammers often employ more diverse and sophisticated tactics, such as phishing emails, fake banking websites, or social engineering techniques.</p>

<p>The transition from in-person to online scams highlights the adaptability of fraudsters and underscores the importance of digital literacy and cybersecurity awareness in the modern age.</p>

</div>