Grande Vista Bay
Newsletter Special Edition
Tech Brief - Social Media, Scams, Internet & More
April 2025

Grande Vista Bay
Newsletter Special Edition
Tech Brief - Social Media, Scams, Internet & More
April 2025

This edition is focused on sharing many types of scams and other issues that are growing by the day.
The more aware you are, the better you can protect yourself.
New Scams and Fraud Schemes appear daily.

Please share with friends and family.

Did You Know?
Scams

National Slam the Scam Day
March 6, 2025

On National Slam the Scam Day and throughout the year, we give you the tools to recognize Social Security-related scams and stop scammers from stealing your money and personal information.

Help protect your loved ones and people in your community this Slam the Scam Day by:

1. **Learning about the latest scams. Information can empower you to quickly recognize a scam. Signs of a scam include:**
   a. **An unexpected problem or offer of a prize or benefit increase,**
   b. **Pressure to act immediately, and**
   c. **A request for an unusual payment like cryptocurrency, gift cards, gold bars, and wire transfers, even with the promise of keeping your money "safe."**
2. **Reporting scams as soon as possible. Victims shouldn't be embarrassed if they shared personal information or suffered a financial loss. We are all vulnerable.**
3. **Sharing our Scam Alert fact sheet and helping educate others about how to protect themselves.**

Report Social Security-related scams to the Social Security Administration Office of the Inspector General (OIG).

Visit www.ssa.gov/scam for more information and follow SSA OIG on Facebook, X, and LinkedIn to stay up to date on the latest scam tactics. Repost #SlamtheScam information on social media to keep your friends and family safe.

Did You Know?
Scams

From Chase Bank ~The latest to know

Nearly 50% of scams reported to Chase originate on social media (but this could be any bank)

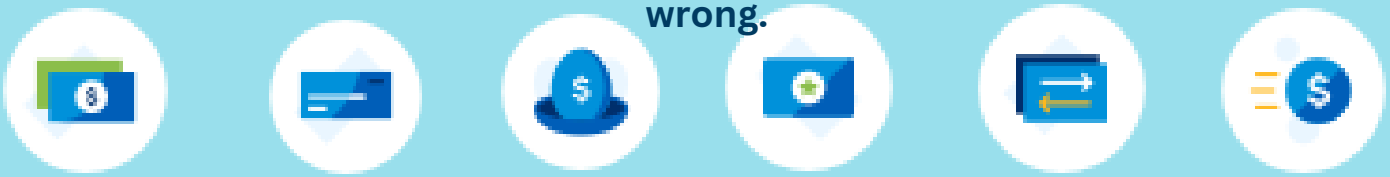
Many of our customers are reporting to us that scammers on social media asked them to send their payment with Zelle® or Wires*

Avoid sellers who require certain forms of payment

These payment types do not have purchase protection. If you use them to pay a scammer you most likely will not get your money back.

Social media is flooded with fake ads for things like merchandise, cars, property rentals and home services. These scams can show up in marketplaces, spoof websites and groups you follow.

Keep in mind that sending money with Zelle® or a Wire transfer is just like sending cash. It's highly unlikely you'll get your money back if something goes wrong.



Cash Checks Crypto Gift Cards Wire Transfers Zelle®

Be alert for fake ads and listings in your social media feed and groups — these are real scams happening now

<u>Deceptive ads</u>

Scammers are advertising on social media with great deals on the hottest items like concert tickets. You pay, but it never arrives.

<u>Shady listings</u>

Social feeds have listings for bogus cleaning and home improvement services. You pay a deposit, no one shows.

<u>Fake profiles in groups</u>

Social media groups show great rental deals. You feel safe sending a deposit because it's posted by a group member, then they vanish.

Did You Know?
Scams - Phone # Porting

9 ways scammers can use your phone number to try to trick you

Don't fall for these phone scams by crooks

Scammers have various methods when it comes to getting their hands on your phone number. You might think, "Well, what's the big deal? Isn't it easy to find someone's number these days, no matter what?" Yes. And if you've already had your fair share of telemarketers call you, maybe you feel like you've got it under control.

The problem is that scammers with the right knowledge and the wrong intentions can wreak havoc just by having your phone number in their possession. Once they do, they can use it to trick you in all sorts of ways.

The good news is that by familiarizing yourself with their tactics, you can be one step closer to preventing yourself from falling victim to them. Here's what you need to know.

9 ways you can get scammed if your phone number falls into the wrong hands

In today's digital age, your phone number is more than just a way for friends and family to reach you. It can be a gateway for scammers to access your personal information and wreak havoc on your life. From phishing attempts to extortion, the risks are numerous and varied. Here are nine ways scammers can exploit your phone number if it falls into the wrong hands:

1. Phishing for other personal information - Scammers can also use your phone number to launch rather easy phishing attacks. They might send text messages or make calls posing as your bank or a popular online service that you subscribe to. The goal is to call you and trick you into providing login credentials, credit card details or other personal information, which they can then use for fraudulent activities. And once they have all your other information, they can do a lot more damage just by having your phone number as that initial segue.

2. Extortion and blackmail - In some cases, scammers use your phone number for extortion or blackmail. They may claim to have compromising information about you and demand payment to keep it private. By contacting you directly, they can apply continuous pressure, making their threats seem more real and immediate. One unique way they do this to target elderly people is by pretending to be your grandchild or another relative in distress. The scammer often claims that your grandchild is in an emergency situation — such as needing bail money or medical assistance — and urgently requests financial help. With AI voice cloning technology, they may even be able to use your grandchild's voice. This emotional manipulation usually gets the victim to pay up.

3. Robocalls and spam messages - This one may not be as dramatic, but your phone number can be sold to robocall and spam message services. These automated systems bombard you with unwanted calls and texts, often promoting scams or fraudulent products. While these may seem like minor annoyances, they can lead to bigger scams if you engage with the messages or follow their instructions. Hang up on them.

Did You Know?
Scams - Phone # Porting

4. Phone number spoofing - Phone number spoofing is a common tactic where scammers disguise their caller ID to appear as a trusted contact by calling from what appears to be a familiar number as it may have the same area code where you live, an area code where your friends or family live or even the actual phone number of someone close which you can recognize.
This makes it more likely that you'll answer the call, giving them the opportunity to deceive you into revealing personal information or transferring money. This is, of course, the case when phone spoofing is used against you. But in situations where they use YOUR phone number, they can be scamming those close to you without you even knowing!
5. Impersonating government agencies - With these phone spoofing tactics, scammers can use your phone number to impersonate government officials, such as IRS agents or Social Security administrators. They may call you claiming there's an urgent issue, like unpaid taxes or suspicious activity involving your Social Security number. This ploy often involves threats of legal action or arrest to pressure you into providing sensitive information or making immediate payments.
6. Calling about fake unpaid invoices - Instead of pretending to be from a government agency, another trick is for scammers to try their luck by posing as a representative from a utility company, like an electric or water company. Scammers will claim that you have an overdue invoice and threaten to cut off your service unless you pay immediately. Using your phone number, they can contact you repeatedly, making the scam seem more legitimate (and pressing).
7. SIM swapping/phone rerouting - SIM swapping or a port-out scam is when scammers transfer your phone number to a new SIM card in their possession. By convincing your mobile carrier to reroute your number, they can receive all your calls and messages, including those containing two-factor authentication codes. This allows them to bypass security measures and take over your online accounts.
8. Stealing your sensitive data - With SIM swapping techniques/port-out, scammers can also use your phone number as a key to access sensitive data stored in your online accounts. By initiating password resets and intercepting verification codes sent via SMS, they can gain unauthorized access to your email, social media and banking accounts, leading to significant personal and financial damage.
9. Setting up fake online accounts - Finally, scammers can use all the tactics above to not only access the accounts you already have but also create fake online accounts in your name. These accounts can be used for a variety of malicious purposes, such as spreading malware, launching further scams or conducting identity theft. The presence of your phone number makes these accounts appear more legitimate, increasing the chances of deceiving others.

Note: this has happened to someone in our neighborhood.

Did You Know?
Scams - Protect Yourself

How To Protect Yourself From These Scams

To protect your phone number from falling into the hands of scammers, here's what you can do:

1. Be cautious about sharing your phone number publicly: Avoid posting your phone number on public forums, websites or social media platforms where it can be easily accessed by scammers.

2. Limit exposure of your phone number on social media and other online platforms: Use privacy settings to restrict who can see your contact information. Most social media platforms and online services offer privacy settings that allow you to control who can view your personal information. Make sure to review and adjust these settings regularly. Only share your phone number with trusted contacts.

3. Consider using a secondary number for online registrations and transactions: Services like Google Voice can provide you with a secondary number that you can use for online activities, keeping your primary number private.

4. Monitor your accounts regularly for unusual activity: Check your bank accounts, email and other online accounts for any signs of unauthorized access or suspicious activity.

5. Have strong antivirus software: The best way to safeguard yourself from malicious links that install malware, potentially accessing your private information, is to have antivirus software installed on all your devices. This protection can also alert you to phishing emails and ransomware scams, keeping your personal information and digital assets safe.

6. Use two-factor authentication apps instead of SMS-based verification where possible: Two-factor authentication (2FA) provides an extra layer of security that is more difficult for scammers to bypass compared to SMS-based verification.

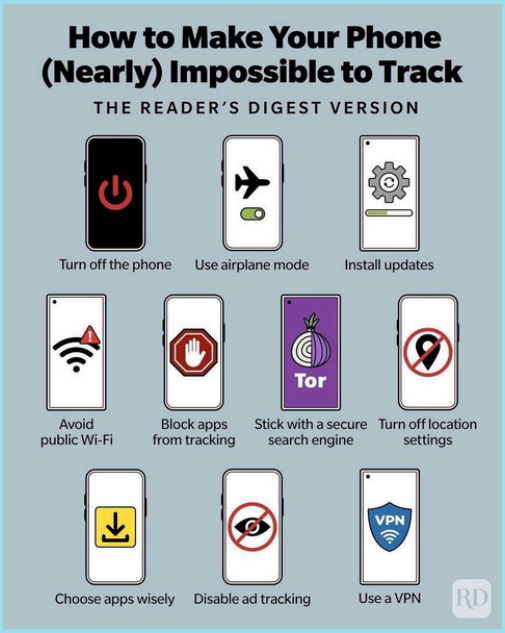
7. Use an identity theft protection service: Identity theft companies can monitor personal information like your Social Security number, phone number and email address and alert you if it is being sold on the dark web or being used to open an account. They can also assist you in freezing your bank and credit card accounts to prevent further unauthorized use by criminals. One of the best parts of using some services is that they might include identity theft insurance of up to $1 million to cover losses and legal fees and a white glove fraud resolution team where a U.S.-based case manager helps you recover any losses. See my tips and best picks on how to protect yourself from identity theft.

Did You Know?
Scams - Protect Yourself

8. Remove your personal information from the internet: While no service can guarantee the complete removal of your data from the internet, a data removal service is really a smart choice. They aren't cheap, and neither is your privacy. These services do all the work for you by actively monitoring and systematically erasing your personal information from hundreds of websites. It's what gives me peace of mind and has proven to be the most effective way to erase your personal data from the internet. By limiting the information available, you reduce the risk of scammers cross-referencing data from breaches with the information they might find on the dark web, making it harder for them to target you.

Contact your mobile carrier to alert them of the scam calls, especially if they come from the same number. Your carrier may be able to block the number or provide additional security measures.

Consider changing your phone number if the issue persists: If scam calls continue despite your efforts, changing your phone number may be the best solution.
Report any suspicious activity to the appropriate authorities: Contact your local law enforcement or consumer protection agency to report scams and seek advice on further actions.
Consider placing fraud alerts on your accounts: Fraud alerts can help protect your credit and financial accounts from unauthorized access.
Monitor your phone for unusual calls or messages: Keep an eye out for any unexpected calls or messages, and do not respond to them.
Check your phone bill for unauthorized charges: Regularly review your phone bill to ensure there are no unexpected charges, which could indicate that your number has been used fraudulently.



Did You Know?
Scams - Smishing

The FBI has issued a nationwide warning about a new wave of "smishing" attacks spreading across the United States

Smishing texts are fraudulent messages sent via SMS (Short Message Service) or text messaging with the intent to trick recipients into revealing personal information, such as passwords, credit card details or other sensitive data.
The term "smishing" is a combination of "SMS" and "phishing," referring to deceptive tactics used to manipulate individuals into providing confidential information.

Cybercriminals have registered more than 10,000 domains to fuel these scams, which target iPhone and Android users with fraudulent text messages designed to steal personal and financial information.

Authorities urge recipients to delete any suspicious messages immediately.

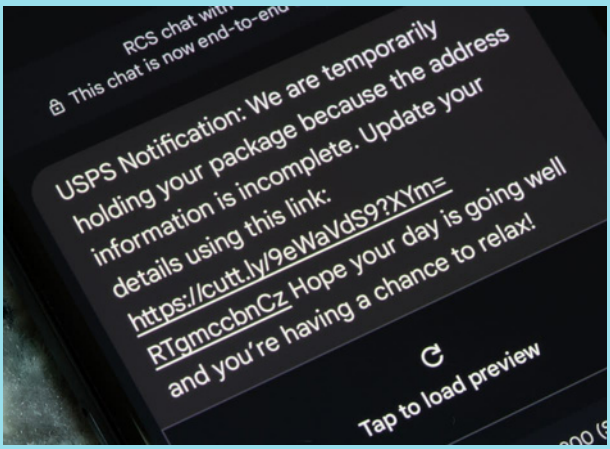
A new report from cybersecurity firm Palo Alto Networks' Unit 42, the company's research division that specializes in threat intelligence and incident response, reveals that these scams lure victims into providing sensitive data, including credit card and bank account details.

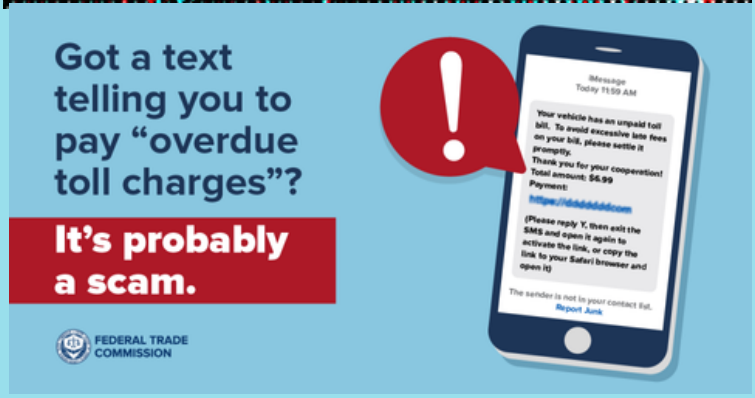
Initially centered on fraudulent toll payment notifications, the campaign has expanded to include fake delivery service alerts, tricking users into clicking malicious links. For months, state and local authorities have been raising alarms about the toll scam, which falsely claims that recipients owe unpaid toll fees. The Federal Trade Commission (FTC) warns that clicking on these links not only risks financial theft but also exposes victims to identity fraud.
The fraudulent messages follow a common pattern: They claim that an unpaid bill requires immediate action to avoid penalties.

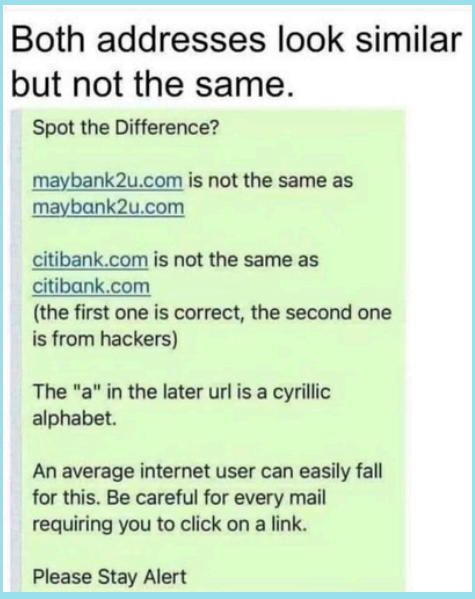
The text includes a link directing users to a payment portal — which is where the scammers' vast network of domains comes into play. Since Apple's iMessage blocks suspicious links, scammers now instruct users to copy and paste the URL into their web browser, making detection harder.
Cybersecurity experts believe that the scam operates as a franchise model, leveraging tool kits from Chinese cybercriminal groups.
Unit 42 identified numerous malicious domains, many using China's .XIN top-level domain (TLD), including:: dhl.com-new[.]xin, fedex.com-fedexl[.]xin, ezdrive.com-2h98[.]xin, e-zpassny.com-ticketd[.]xin, sunpass.com-ticketap[.]xin, thetollroads.com-fastrakeu[.]xin.

The FTC advises that legitimate US toll services and delivery companies would never redirect users to foreign domains or foreign phone numbers. .

Did You Know?
Scams & Smishing







USPS

Consumers are now being scammed by text messages claiming that a USPS package is undeliverable due to an invalid ZIP code. The fraudulent links in smishing texts may install malware or redirect users to fake websites that harvest sensitive data, according to the U.S. Postal Inspection Service.

Did You Know?
Scams - Smishing

United States Postal Service - USPS

The U.S. Postal Inspection Service's new tips for avoiding scams coincide with the rise of a scheme that targets consumers through fraudulent text messages impersonating the U.S. Postal Service.

Why It Matters

Americans lose billions of dollars each year to scammers. Roughly $8.8 billion was stolen due to fraud in 2022, according to the Federal Trade Commission.

What To Know

Fraudulent messages, known as "smishing" scams, are a growing threat. Smishing is a form of phishing that involves text messages designed to steal personal information. These messages often impersonate trusted entities like government agencies or banks, attempting to trick recipients into revealing account credentials, Social Security numbers, or financial details.

Consumers are now being scammed by text messages claiming that a USPS package is undeliverable due to an invalid ZIP code. The fraudulent links in smishing texts may install malware or redirect users to fake websites that harvest sensitive data, according to the U.S. Postal Inspection Service.

The USPIS, the self-described "law enforcement arm of the U.S. Postal Service," aims to secure the nation's mail system.
As part of the grassroots campaign National Consumer Protection Week, which runs March 2 to 8, the USPIS has launched an informational page detailing how to identify and avoid scams.
The U.S. Postal Service (USPS) has released a podcast on imposter scams, which discusses real-life scam cases and provides prevention tips.

USPIS officials stress that the USPS does not send unsolicited text messages about delivery problems. In a press release, Eric Shen of the USPIS Criminal Investigations Group emphasized that scammers "lull consumers into a false sense of trust, gain access to privileged information, and then drain financial accounts."

Did You Know?
Scams - Smishing

United States Postal Service - USPS

What Does The USPS Scam Text Say?

One USPS scam text obtained by Newsweek reads: "USPS package has arrived at the warehouse and could not be delivered due to an invalid zip code address being detected. Please confirm the zip code address information link."

The message contains a fake link that, when clicked, can compromise users' personal information.

Security experts warn that scammers frequently change their messaging tactics, but red flags often include poor grammar, a sense of urgency, and links that do not direct to official USPS domains.

What To Do If You Receive a Scam Text

The USPIS advises consumers to take the following steps if they receive a suspicious text message:

- **Do not click any links or respond to the message.**
- **Report the scam by forwarding the text to 7726 (SPAM).**
- **Report to USPIS by emailing spam@uspis.gov with a copy of the message and a screenshot showing the sender's number and date sent.**
- **Block the sender on your phone to prevent future messages.**
- **Verify tracking information by visiting the official USPS website rather than clicking on links in messages.**

Consumers who believe they may have fallen victim to a scam should immediately contact their bank or credit card provider to secure their accounts and monitor for fraudulent activity.

Did You Know?
Scams - Virus Warning

WARNING VIRUS DETECTED Computer Scam
DO NOT CLICK ON ANYTHING ON THE SCAM NOTICE

The “Warning! Virus Detected” pop-up is a push notification that uses fake alerts stating that your device is under attack or infected to trick you into clicking on it.

Cyber Security Tip: If this type of alert pops up, DON’T click on it! ========== You’re working at your computer when suddenly – BAM! – you get a pop-up notification that your PC is infected with a virus and you must “click here” to run a scan or install antivirus software.

This is a common scareware tactic used by hackers to get you to click and download a virus. (You should know we would NEVER deliver that type of pop-up to you!) Often it will appear to be a system alert or a Microsoft operating system alert. Regardless of how legitimate it looks, NEVER click on the site or the pop-up.

The safest thing to do is close your browser; do not click on the X, “Close” or “Cancel” button in the pop-up or on the site because clicking on anything on the page or pop-up will trigger a virus download.
If that won’t work, bring up your task manager (hold Control + Alt + Delete on a PC and Command + Option + Esc to “Force Quit” on a Mac) and close the web browser or application where the alert appeared.

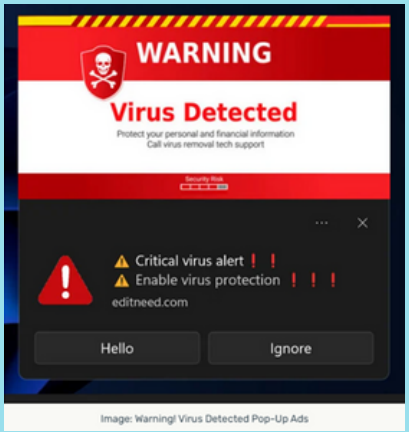


Image: Warning! Virus Detected Pop-Up Ads

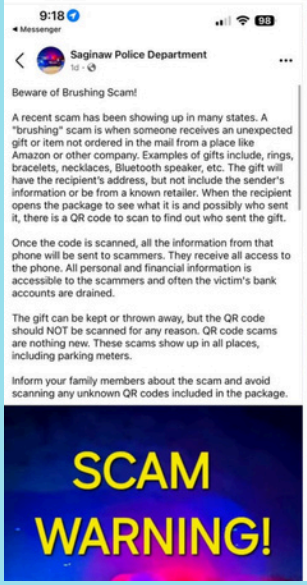
Example

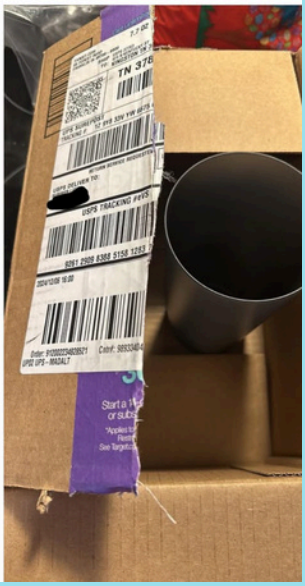
Did You Know?
Scams

BEWARE, Don't fall this very sophisticated debit card scam. Here's how it goes: got a call, the caller ID was my bank. The guy says he's from the fraud dept, calling about my debit card ending in ----(the 4 correct numbers), and asks if i'd been traveling, reports 2 suspicious charges that happened at out-of-state stores (Lowe's and Walmart). I said nope, wasn't me. He says they'll send me a new card. He knows my address. He knows all my phone numbers. He sends a verification code to my cell and asks me to read it to him. THEN HE ASKS FOR MY PIN NUMBER, so he can deactivate it. That's where I said "no." But he has an answer for my suspicions: he says look at the number I'm calling from, it matches the number on the back of your card. It does! But still, then I said let me call you back and he hung up! I reported this to my bank's fraud dept, who said WE WOULD NEVER ASK FOR YOUR PIN NUMBER. (And immediately cancelled my card.) They also said this is the new scam, they're hearing about it a lot. Tell everyone!

If you get a call from TVA credit Union saying your card was stolen. Hang up and call them back yourself. People are spoofing their phone number and claiming your card was stolen. They will ask if you want to cancel it, then they will then start telling you your information address exc. And some of the digits of your card before asking for you to confirm the rest. They are good but they didn't get me. It was just a little bit of a different call then I have had from from TVA in the past. So be careful and just call them back on a known number if you get a call. I called and they confirmed it was scam and happening a lot right now.

‼️It's REAL! I had a package delivered to me a few days ago. It was addressed to me as well. It was in a target box. When I opened it, it was just a plastic cup. There was also a QR code sticker on the bottom of the cup. Thank God I didnt click it! I also called target and they couldn't find anything that was shipped out to me. ‼️ Just a heads up for anyone that receives an unexpected package!

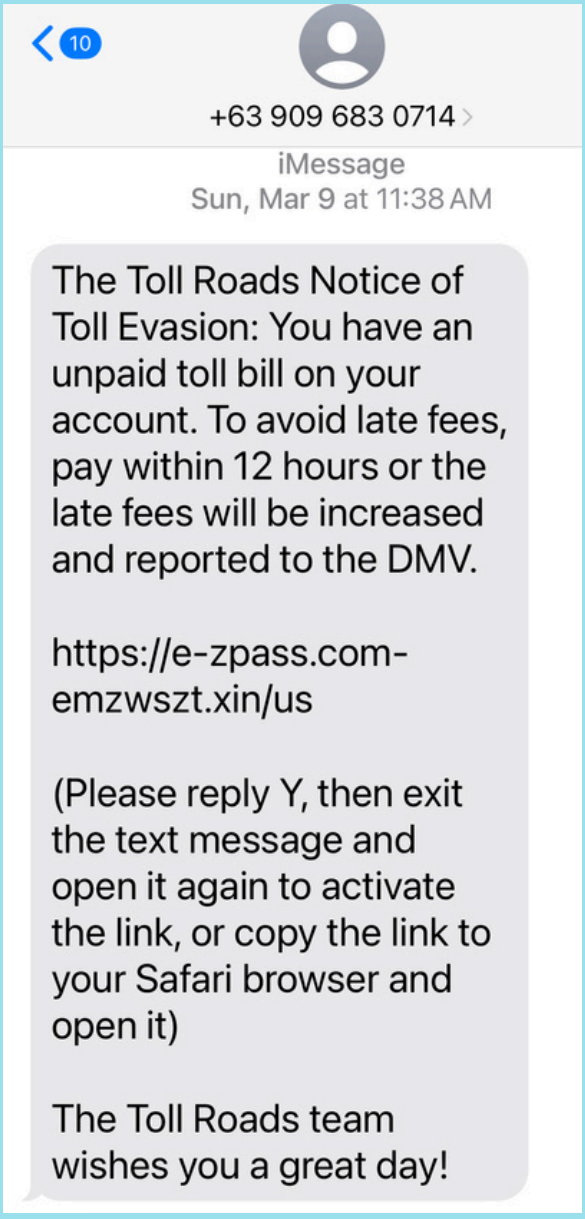




Did You Know?
Scams

🚨 **BREAKING: If you receive a text saying that you have unpaid tolls, do not click on the link. It's a nationwide scam. Report as spam and delete.**

This is a real text.
Note that it is from an international phone #; not a US phone #.
The recipient had not been out of the country; nor had they been on any toll roads.
But these toll scams can come from anywhere!
DO NOT REPLY.
DO NOT CLICK ON A LINK.
DELETE ALL OF THESE YOU RECEIVE!



Did You Know?
Scams

myTDOT
1h ·

SCAM ALERT. TDOT is aware of text messages claiming people have unpaid toll road charges and potentially implying the message is coming from TDOT. THIS IS A SCAM. There are no toll roads in Tennessee. The FBI says it's part of a scam growing nationwide and urges people not to click on any links connected to these texts.

Trying to figure out how people have “unpaid toll road charges” when there are ***NO TOLL ROADS IN TN.***

Trying to figure out how people have “unpaid toll road charges” when there are ***NO TOLL ROADS IN TN.***

Did You Know?
Scams

Warning 🚨 My nephew and his girlfriend went to Meijer Friday night it was late they are young and apparently didn't notice anything or anyone following them, however at some point and time once home they noticed a zip tie was placed on their front driver's side rim. They took a picture and my sister notified the Mooresville police. They came out and let them know that sex traffickers and drug traffickers place this on victims tires sometimes it can be laced with fentanyl to make the victims pass out so they can take them. They let her know to never remove it because that gives them time to kidnap them. Please if you have young daughters who drive make them aware and tell them to always watch their surroundings. This is scary and too close to home!

10 most common scams on social media [2]

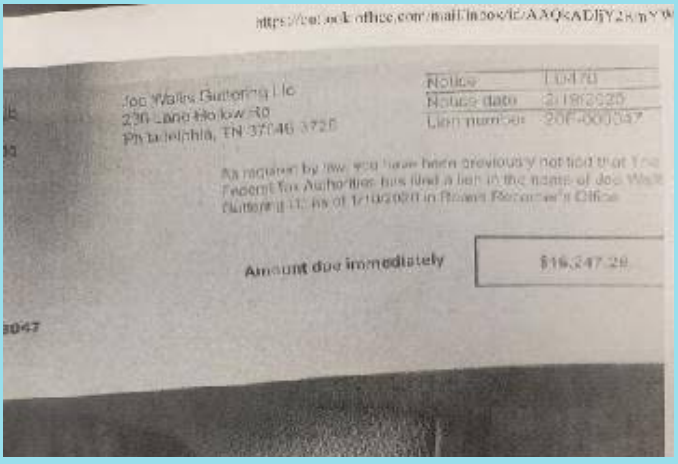
1. Tickets
2. Property rentals, sales or leases
3. Car / Car Parts
4. Puppies / Pets
5. Furniture
6. Electronics
7. Moving / Shipping
8. Clothes / Jewelry
9. Home contractors
10. Household appliances

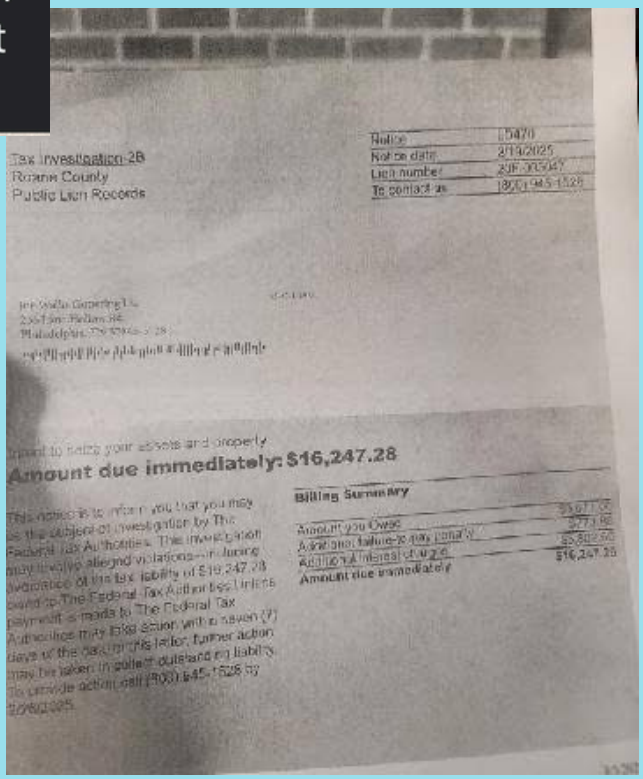
Did You Know?
Scams

Roane County Sheriff's O...
4h ·

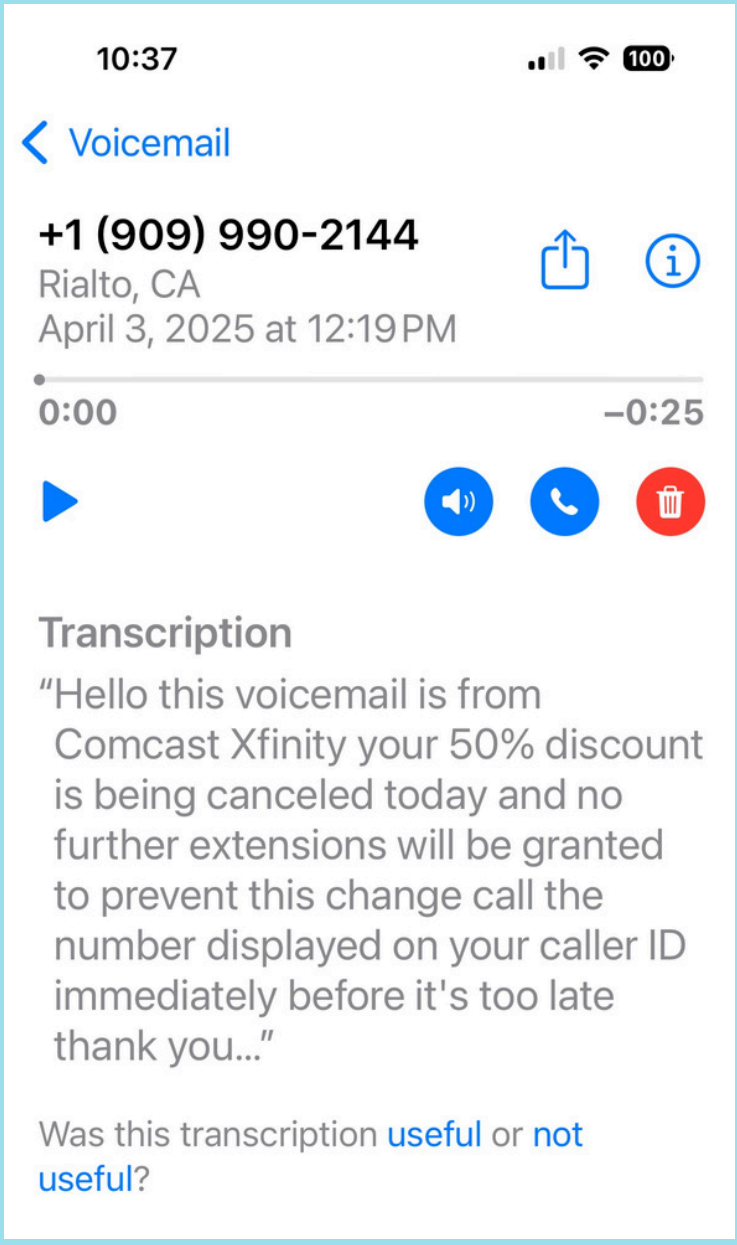
SCAM WARNING

A Roane County resident recently reported to us that they received a letter allegedly from the Property Assessors office, informing them that they needed to pay over $16k in taxes and penalties on their commercial property, threatening to seize the property if they did not comply. The resident was suspicious of the letter and contacted the local PA office, who confirmed that it was in fact a scam. If you receive a letter like this, do not send any money or provide any information. You can call 865-376-4362 to verify any document you receive.





Did You Know?
Scams



This is a real Voicemail message

Notable scam identifiers:

- "Comcast Xfinity" not Xfinity - They no longer use the name Comcast
- Call the # on caller ID; didn't say call Xfinity
- Came from Area Code 909 (LA area); not a normal 800 series
- Offering a "Discount" that is not real and you did not have
- Note that it is being "cancelled" - not that the discount period ended
- Notice the urgency – "immediately" like it is an emergency

Did You Know?
Scams - AI Generated

GenAI, the future of fraud and why you may be an easy target
AI fraud: What you need to know and how to stay safe

By Kurt Knutsson, CyberGuy Report

"Mom, it's me! I've been in an accident and need money right away!"

The voice on the phone sounds exactly like your child, but it's actually an artificial intelligence clone created from a three-second clip of his voice on Facebook. Welcome to the frightening new world of AI-powered fraud. Generative artificial intelligence (GenAI) has handed scammers a powerful new toolkit that makes yesterday's email scams look amateur by comparison.

The sophisticated fraud techniques emerging today are virtually undetectable to the untrained eye, or ear. And the financial impact is staggering. Since 2020, phishing and scam activity has increased by 94%, with millions of new scam pages appearing monthly. Even more alarming, experts estimate losses from AI-powered scams will reach $40 billion in the U.S. by 2027.

What is generative AI and why should you care?

Generative AI refers to so-called artificial intelligence systems that create new content — text, images, audio or video — based on data they've been trained on. Unlike traditional AI that analyzes existing information, generative AI produces entirely new, convincing content. The most concerning part? These powerful tools are increasingly accessible to fraudsters who use them to create sophisticated scams that are harder than ever to detect.

How fraudsters are weaponizing GenAI

Today's scammers use generative AI to "supercharge" their existing techniques while enabling entirely new types of fraud, according to Dave Schroeder, UW–Madison national security research strategist. Here are the four most dangerous ways they're using this technology.

Voice cloning: The 3-second threat

With just three seconds of audio, easily obtained from social media, voicemails or videos, fraudsters can create a convincing replica of your voice using AI. "Imagine a situation where a 'family member' calls from what appears to be their phone number and says they have been kidnapped," explains Schroeder. "Victims of these scams have said they were sure it was their family member's voice." These AI-generated voice clones can be used to manipulate loved ones, coworkers or even financial institutions into transferring money or sharing sensitive information, making it increasingly difficult to distinguish between genuine and fraudulent calls.

Did You Know?
Scams - AI Generated

Fake identification documents

Today's AI tools can generate convincing fake identification documents with AI-generated images. Criminals use these to verify identity when fraudulently opening accounts or taking over existing ones. These AI-generated fake IDs are becoming increasingly sophisticated, often including realistic holograms and barcodes that can bypass traditional security checks and even fool automated verification systems.

Deepfake selfies

Many financial institutions use selfies for customer verification. However, fraudsters can take images from social media to create deepfakes that bypass these security measures. These AI-generated deepfakes are not limited to still images; they can also produce realistic videos that can fool liveness detection checks during facial recognition processes, posing a significant threat to biometric authentication systems.

Hyper-personalized phishing

Similarly, GenAI now crafts flawlessly written, highly personalized phishing emails that analyze your online presence to create messages specifically tailored to your interests and personal details. These AI-enhanced phishing attempts can also incorporate sophisticated chatbots and improved grammar, making them significantly more convincing and harder to detect than traditional phishing scams.

Why you might be a prime target

While everyone is at risk from these sophisticated AI scams, certain factors can make you a more attractive target to fraudsters. Those with substantial retirement savings or investments naturally represent more valuable targets — the more assets you have, the more attention you'll attract from criminals looking for bigger payoffs. Many older adults are particularly vulnerable as they didn't grow up with today's technology and may be less familiar with AI's capabilities. This knowledge gap makes it harder to recognize when AI is being used maliciously. Compounding this risk is an extensive digital footprint: if you're active on social media or have a significant online presence, you're inadvertently providing fraudsters with the raw materials they need to create convincing deepfakes and highly personalized scams designed specifically to exploit your trust.

How to protect yourself in the age of AI

Protection against AI-powered threats requires a multi-layered approach that goes well beyond just digital measures. Awareness is your first line of defense — understanding how these scams work helps you spot red flags before you become a victim. This awareness should be paired with both digital safeguards and "analog" verification systems that exist entirely offline. Here are some key steps to protect yourself:

Did You Know?
Scams - AI Generated

1. Invest in personal data removal services: Generative AI fundamentally needs your personal data to craft convincing scams, which is why limiting your online footprint has become paramount in today's fraud landscape. The less information about you that's publicly available, the fewer raw materials scammers have to work with. Going completely off-grid is unrealistic for most of us today — much like never leaving your home. But you can reduce your online footprint substantially with a personal data removal service like Incogni, making yourself significantly less exposed to AI-powered scams.

By removing your personal data from data broker companies, you not only protect yourself from GenAI-powered fraud but also gain numerous other privacy benefits, such as reduced risks of receiving spam and falling victim to identity theft, as well as helping to prevent stalking and harassment. As AI technology advances, gen-AI scams will only become more sophisticated. While no service promises to remove all your data from the internet, having a removal service is great if you want to constantly monitor and automate the process of removing your information from hundreds of sites continuously over a longer period of time.

2. Establish your own verification protocols: Consider agreeing on a "safe word" that only family members know. If you receive an unexpected call from a relative in distress, ask for this word before taking action.

3. Choose strong, unique passwords for each account: Create complex passwords using a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like birthdays or common words. Consider using a password manager to generate and store complex passwords. A password manager can generate and store strong, unique passwords for all your accounts, reducing the risk of password reuse and making it easier to maintain good password hygiene.

4. Enable two-factor authentication (2FA) on all accounts: 2FA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, in addition to your password.

5. Receive MFA codes via an authenticator app on your phone rather than email when possible: Using an authenticator app like Microsoft Authenticator or Google Authenticator is more secure than receiving codes via email. Authenticator apps generate time-based one-time passcodes (TOTPs) that are not transmitted over email or SMS, reducing the risk of interception by hackers. Additionally, authenticator apps often support biometric authentication and push notifications, making the verification process both secure and convenient.

Did You Know?
Scams - AI Generated

6. Use a strong antivirus software: Modern cybersecurity threats are evolving rapidly, with AI being used to create more convincing phishing attacks, deepfake scams, and malware. Investing in strong antivirus software can help identify and block suspicious activity before it reaches you. The best way to safeguard yourself from malicious links that install malware, potentially accessing your private information, is to have strong antivirus software installed on all your devices. This protection can also alert you to phishing emails and ransomware scams, keeping your personal information and digital assets safe.

7. Trust your intuition and verify: If something feels "off," like you notice unusual phrasing or strange background noises, trust your instincts. Don't let fraudsters create a false sense of urgency. If you receive a communication claiming to be from a financial institution, call that institution directly using the official number from its website.

8. Monitor your accounts: Review account statements regularly for suspicious transactions. Don’t hesitate to request a credit freeze if you suspect your data has been compromised.

SUBSCRIBE TO KURT’S YOUTUBE CHANNEL FOR QUICK VIDEO TIPS ON HOW TO WORK ALL OF YOUR TECH DEVICES

https://cyberguy.com/Newsletter/
https://www.facebook.com/CyberGuyOfficial/

Kurt's key takeaways

So, is this all a bit scary? Absolutely. But the good news is, you're now armed with the knowledge to fight back. Stay alert, take those protective steps I mentioned seriously, and remember that a little healthy skepticism goes a long way in this new age of AI fraud. Let's make it much harder for these AI-powered scams to succeed.

Did You Know?
Scams

Residents concerned about "X" markings on cars

NASHVILLE, Tenn. (WSMV) - There are growing concerns about white “x” markings popping up on cars. Two women who spotted them shared why the markings sparked worry and what police said they could mean.

One woman said she parked her car outside of her Madison apartment Saturday night and on Sunday morning she saw something strange.

“I noticed it before I even got to press the button to open my car,” Natasha Reynolds-Semafumu said.

Reynolds-Semafumu said she spotted a white “X” drawn on her back windshield.

“I took a picture of it, tried to scrape it off but it didn’t come off,” Reynolds-Semafumu said.

That’s when she said panic shot through her body, so Reynolds-Semafumu posted the picture to this Nashville girls' group Facebook page and called 9-1-1.

“There are other girls who have had similar things happen,” Reynolds-Semafumu said.

Sarah Baldwin was one of the women who commented on the post and said her heart dropped when she saw the mark on Natasha’s post.

“That anxiety and fear just a came over again,” Baldwin said.

Baldwin said her car was marked a few years ago in a shopping center parking lot after seeing two people watching and following her.

“My younger sister was with me, and we rushed in and the line was ridiculous and something in me just said we should stay inside the store,” Baldwin said.

And tonight, growing concerns about white X markings popping up

But, when she and her sister came back out to their car, they found a marking on the car window and quickly called the police.

“Officers brought me in and searched the vehicle for any bugs or any tracking device and said that there are numerous cases now that are coming up,” Baldwin said.

Baldwin said MT. Juliet’s police officers told her these were markings for sex traffickers.

The Mt. Juliet Police Department confirmed investigating an incident involving “X” markings but found no evidence linking the mark to sex trafficking.

“No current or past investigations across Tennessee have identified a trend involving “X” markings,” explained MJPD Deputy Chief Tyler Chandler.

Reynolds-Semafumu said Metro Police gave her a slightly different explanation and inferred the mark could be linked to car thefts.

“It’s a marker of something. It just kind of scared me now. I’m afraid to let my kids outside,” Reynolds-Semafumu said.

While Metro Police said they’re continuing to look into what these markings mean, Reynolds-Semafumu is warning people in the area to stay alert.

Did You Know? Passwords

Passwords

A complex password is a necessity but hard to remember. And with so many websites requiring a password these days, users often reuse the same password again and again with different sites. bad idea.

When a big company gets hacked (like LinkedIn, for example), the criminals post and sell the username, e-mail, password and confidential information in that account. Since many people reuse the same password, hackers will try that e-mail and password combination across multiple sites, including Amazon, PayPal or other sites where you might store credit card information.

Remember, they aren't doing this manually. They have highly sophisticated software to automate all of this. If you want a better way of storing and organizing unique passwords, we recommend using a password management system. Do not store your passwords in Excel files, Word files or within your Outlook. These are super easy for attackers to break into.

The bottom line is that no matter how much of a pain it is, it is very important to have different passwords for each online account – and make sure they are truly unique, not just with a system like using the first letter of the site or simply adding "1" or an "!" as an extra character. Hackers will often get access to multiple passwords at once and these patterns become obvious very quickly.

A weak password is still the #1 way hackers break into your network. In fact, 81% of the total number of breaches last year utilized weak or stolen passwords!

Here's what a GOOD password should contain:

- A minimum of eight characters
- Uppercase and lowercase letters
- At least one number and one symbol (#, for example)
- No complete words, like "PaSsWord123#." While this meets the requirements, a hacker's brute-force software will crack that in seconds.
- Never reuse a password for multiple accounts (like making your Facebook and LinkedIn passwords the same).

Did You Know?
Web Browsers

Web Browsers

To limit the data gathered on you when surfing the web, trade in your current browser for DuckDuckGo.

Unlike Google and Bing, DuckDuckGo doesn't track you online, your history and searches, linking them back to you.

It also won't serve up targeted ads based on your private searches. Of course, that will limit some of the features of the browser, but if privacy is important, then this is the best search engine to use.

Who are you?

The hackers and scammers will figure it out.
Social engineering is big business. What is it? Figuring out who you are and then using that information to make money off it.

People list password challenge and identity verification publicly on their Instagram, Twitter and Facebook pages and feeds without giving it a second thought. Maiden name? Check. Favorite pet? Check. High school? Check. Town they grew up in? Check. Favorite or first car? Check. Throwback Thursday is a social engineer's dream! They love this stuff.

Combat this by a) not posting that information online anywhere, or b) always giving false password and identity challenge and verification information to the sites and services that require it. Keep the answer file offline. Remember, if it's a handwritten list, you can still take a photo of it.

Super tip: update your Facebook birthday. Consider having a fake birthday that you use on social media. Not only will this help you identify who is just saying happy birthday because Facebook reminded them...it will also ensure that if someone scrapes your Facebook page, they don't have updated information.

Did You Know?
Tech 4, Donate Computers & Life Step

Donate Your Used Computers & Electronics!

Got old laptops, desktops, or accessories gathering dust? Give them a second life by donating to Tech 4 All Tennessee! We refurbish and distribute devices to individuals in need—helping **them gain access to education, job opportunities, and essential digital skills.**

How It Works:

✅ **Donate** – Drop off your used electronics at one of our Tennessee locations.

✅ **Refurbish** – Our tech team securely wipes data, repairs, and upgrades the devices. 🔐 Secure Data Destruction Guaranteed!

✅ **Empower** – Refurbished devices go to students and individuals in need, bridging the digital divide!

What We Accept:

- 💻 Laptops & desktops
- 📱 Smartphones & tablets
- 📺 Televisions & audio/video systems
- 🖨️ Printers, copiers, & scanners
- 🎧 Accessories & peripherals
- 🔋 Batteries & more!

📍 **Drop-off Locations Across Tennessee:** Harriman, Knoxville, Cookeville, Crossville, Oak Ridge, Alcoa, Rockwood, Chattanooga, and more!

📍 **Find a Drop-off Location:** https://tech4alltn.org/donate-your-used-computers-electronics-and-accessories/

📍 Contact us: info@tech4alltn.org

LIFE-STEP

Life Skills & Tech Empowerment Program

FREE laptop to use and keep after completing 15 hours of training

STEP 1

FOUNDATIONAL SKILLS TRAINING:

- ***Personal Development & Life Skills***
- ***Etiquette & Professionalism***
- ***Computer Skills Training***
- ***Job Readiness, Resume Building***
- ***Health, Wellness & Financial Tools***

More Info @Tech4AllTn.org

email: life-step@tech4alltn.org
call: 865-368-3458

A collaboration of
Tech 4 All Tennessee & P31FS

Rewired for Success: Karsyn's Journey with Tech 4 All Tennessee

The computer refurbishing and training program created by Harriman non-profit Tech 4 All Tennessee is helping to improve the lives of young people in East Tennessee on multiple levels.

Karsyn Davis, 30, is pursuing a degree as a Medical Administrative Assistant at TCAT (Tennessee College of Applied Technology) in Harriman. She credits Tech 4 All Tennessee with helping bring her to a better place in her life.

Just a couple of years ago she felt she was at a low point. "I lost my job and didn't have a car to get to work," she said.

With her marketable job skills limited mostly to retail and fast food, she knew she needed more training. She heard about the opportunity to get a free Chromebook and training from Tech 4 All Tennessee. After completing the program, she connected with Tech 4 All Tennessee Executive Director Dayle Beyer. Beyer asked her to become more involved in the Tech 4 All Tennessee Digital Lab that refurbished computers that are distributed free to the community.

"I learned the refurbishing process for the equipment that we were distributing to the community," Davis said.

She also attended more of the basic computer skills classes as an assistant instructor. Over the following months she progressed to become an instructor of both the 3-hour and more advanced 15 hour classes.

Working at the Digital Lab, Karsyn also learned more about the process of collecting and distributing technology. "I'm getting a lot of experience managing inventory," she said.

She created a Pop-Up-Shop to sell donated items including coffee makers back to the community to fund the program. "We were able to put money back into the lab," she said.

She began attending Tech 4 All Tennessee board meetings to learn more about the organization's management and decided to pursue an Associate Degree at TCAT. "Having someone to mentor me gave me the push to go to school," she said.

Her training at TCAT resulted in her completion of multiple Microsoft certifications that have been added to her resume.Davis said she is also encouraged by knowing that while she learns new skills she is also helping her community and meeting new people. **"It's expanded my world,"** she said.

Tech 4 All Tennessee is a non-profit community-based leader in digital literacy and technology access. We provide free refurbished computers and deliver essential and advanced digital skills training through programs like **Tech Goes Home, Life-Step Foundations,** and the **Digital Lab.** Whether you're a **learner, volunteer,** or **supporter,** we offer real pathways to **opportunity, connection, and growth.**

Join us today and be part of building a more connected, empowered East Tennessee.

tech4alltn.org info@tech4alltn.org (865) 316-6050

Did You Know?
Property Scams & Fraud Schemes

SHARON BRACKETT
ROANE COUNTY REGISTER OF DEEDS
200 E. Race Street, Suite 6, P.O. Box 181
Kingston, Tennessee 37763
865-376-4673

BEWARE

I, Sharon Brackett, the Roane County Register would like people that have recently acquired property in Roane County to be aware that in a few weeks you will receive a solicitation letter from various companies offering to sell information and copies of your deed to you at an inflated price. The same information is available to the public at the Roane County Register of Deeds Office for a minimal copy fee of 15 ¢ per page for most documents.

It appears that individuals who have recently acquired property are the primary targets of these companies. One solicitation states in the fine print that a copy of the party's deed can be obtained from the county recorder in the county where the property is located for a fee up to $123.00. It goes on to recite that the company is not a government entity, but the letter looks very official. When I was contacted by a citizen who had received one of these letters, I contacted the local newspaper to publish a press release informing the public of this solicitation.
Please be aware and we once again urge individuals to please call the Roane County Register's office before sending any money to anyone requesting a charge for a copy of their deed or property profiles.

Property Fraud Alert

The service immediately notifies you if a document is filed under your name or business, allowing you to recognize and stop fraudulent actions instantly.
Property Fraud Alert is a free service that will provide peace of mind by allowing:

- **Instant notification of document filings**
- **24/7 monitoring**
- **Monitoring of multiple names**

This free service became available to the public July of 2021.
Go to: www.roanecountytn.gov
Click on tab: Departments
Look for: Register of Deeds
Red Fraud Alert Tab

Did You Know?
Social Media

What is Social Media?

“Social media, a form of mass media communications on the Internet (such as on websites for social networking and microblogging) through which users share information, ideas, personal messages, and other content (such as videos). Social networking and social media are overlapping concepts, but social networking is usually understood as users building communities among themselves while social media is more about using social networking sites and related platforms to build an audience.”

How does Social Media affect your neighborhood?

“Neighborhood social networks, led by platforms like Nextdoor, have the potential to enrich community life by fostering connections, sharing information, and enhancing civic engagement. The good aspects, including community bonding, local business empowerment, and information sharing, can significantly enhance the quality of life for residents and foster a more connected society.

However, as we have explored, these benefits come with unintended consequences. Privacy concerns, online harassment, localized polarization, and issues related to exclusion and inequality highlight the darker side to these platforms. Furthermore, the potential for exacerbating societal tensions and the specter of commercial exploitation create an urgent need for users, community leaders, and platform creators to address these challenges proactively.

As we navigate the evolution of digital neighborhood engagement, it’s crucial to strike a balance that enhances community ties while safeguarding against the pitfalls these networks can present. Communities must remain vigilant, ensuring their online interactions contribute to the fabric of their neighborhoods rather than tearing it apart. Through conscious effort and critical discourse, neighborhood social networks can become true tools for empowerment rather than division, transforming the way we connect with one another on a hyper-local level.”

Did You Know?
Social Media

How does or has Social Media affected your neighborhood?

What is NextDoor?

"Nextdoor is a **hyperlocal social networking service for neighborhoods**. It was founded in 2008 and is based in San Francisco, California. The platform allows neighbors within the same geographical area to share information and communicate. Neighbors around the world turn to Nextdoor daily to receive trusted information, give and get help, get things done, and build real-world connections with those nearby — neighbors, businesses, and public services."

"Get the most out of your neighborhood with Nextdoor. It's where communities come together to greet newcomers, exchange recommendations, and read the latest local news. Where neighbors support local businesses and get updates from public agencies."

Nextdoor PROS:

- Nextdoor will mail out postcards to all of your neighbors inviting them to join your new group.
- You can chat up community events like garage sales or pool parties.
- It is easy to search for help and give contractor recommendations.
- Your neighbors will help you find your lost pet.
- It's a great way to buy or sell a piece of furniture or accessory or automobiles without having to leave your house.
- You may be able to catch a thief easier.
- You will know more about your community.

Nextdoor CONS:

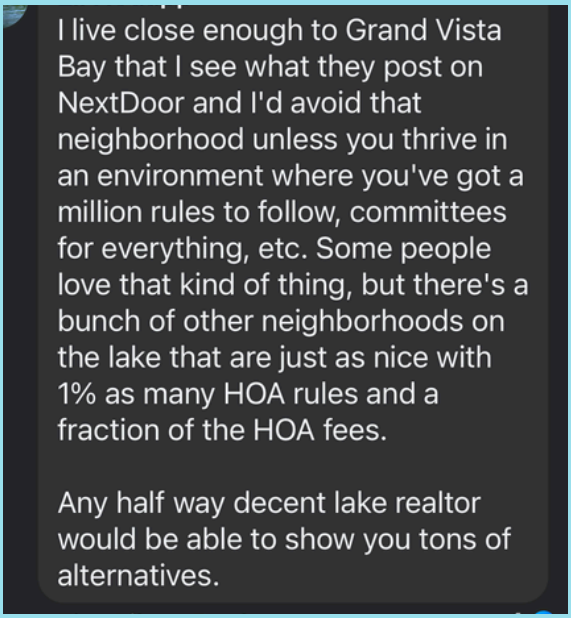
- People share way too much, and many times, things get ugly.
- **Rumors about the community, that in most cases, are not based in fact do more harm than good.**
- Personal disputes get aired publicly. The moderator may allow inappropriate posts to remain out of neglect or they agree with the bully.
- Do you really want other users to know that much about you?
- You will be disappointed in the uncharitable things folks say.
- And Privacy may become a big issue.
- **Nextdoor owns everything you post even if you delete your account.**

Did You Know?
Social Media

How does or has Social Media affected your neighborhood?

Perception & Optics

Reminder: NextDoor is not a personal Facebook or social media page. It is a neighborhood information site. Your neighborhood is a reflection of what you post and how you portray your neighborhood.



This is from an opinion piece about Nextdoor: "Nextdoor, the social media site that allegedly is intended to bring "neighbors" together to discuss local issues and concerns, is more of a bully pulpit.... . The Nextdoor site often portrays communities in the worst possible light, causing negative impacts of property values. It is a bad place to publicly engage."

Opinion: Bullies and cliques plague Nextdoor Social Media site

by Garret Sowards June 26, 2024

This is a sample of the impact NextDoor posts have on the community. This was a post on Facebook where a person said she was coming to town to look at properties and specifically GVB properties. She wanted to know what people liked about GVB and what other developments were in the area. The person who wrote the bit above about GVB lives off of Loop Rd near GVB. He has followed GVB since moving here and often expresses his perception of GVB on both NextDoor and Facebook and usually not in a positive way. Note that he specifically says that he watches what GVB posts on NextDoor. It is up to the community to carefully reflect how posts will impact the community and the perception of the community.

https://machronicle.com/nextdoor-app-is-not-always-so-neighborly/Add a little bit of body text

https://umatechnology.org/nextdoor-and-more-the-good-bad-and-ugly-of-neighborhood-social-networks/

Did You Know?
Windows 10 is End of Service

Outdated PCs put your home & business at risk

Upgrade before support ends for Windows 10 on October 14, 2025. When support ends, you'll no longer receive Windows feature and security updates, which could potentially put you at risk.

- **Set the pace with faster performance**
- **Stay up-to-date and protected against evolving threats**
- **Make the move to supercharged efficiency now**
- **Easy to deploy, compatible with existing tech**

More is possible with Windows 11

This is the best Windows made better, with a Copilot for every person on every device. From AI-powered features to built-in security protections and state of the art creativity, it's the Windows you know, and more.

Easy to deploy, compatible with existing tech

You can upgrade your existing eligible PCs or move to new Windows 11. Options include Copilot+ PCs3, the fastest, most intelligent and secure Windows ever. Rest easy knowing that Windows 11 is designed for compatibility with your existing apps and hardware, making it simple to deliver AI enhanced productivity right away.

You can also use the same deployment tools and strategy that you used for Windows 10.

For more information regarding EOS for Windows 10 and preparing for your upgrade to Windows 11 Pro, here are a few helpful resources:

In Preparation and guidance:

- **Step-by-step deployment best practices and guidance on Microsoft Learn.**
- **Plan for Windows 10 EOS with Windows 11, Windows 365, and ESU**
-

Windows 11 Pro PCs are your foundation for future innovation. Time is running short so get started today.