Scammers Are Getting Smarter – Don't Fall for These New Fraud Tactics!

Fraud isn't new, but the tactics scammers use are evolving faster than ever. Every day, new schemes pop up, designed to trick even the savviest individuals into giving away their personal information or money. The truth is, no one is immune—scammers rely on urgency, fear, and deception to get what they want.

Two scams that have been spreading rapidly involve fake Microsoft pop-ups and scam texts about unpaid tolls. These tactics are deceiving thousands of people, but by understanding how they work, you can stay ahead of the fraudsters.

The Fake Microsoft Pop-Up Scam

You're browsing the internet when suddenly, a pop-up message fills your screen. It warns that your computer is infected with a virus and that immediate action is required. A phone number for "Microsoft Support" appears, urging you to call before your data is lost forever.

Many people panic in this moment—after all, no one wants their computer to crash. But here's the truth: Microsoft will never send security alerts via pop-ups. This is a scam designed to scare you into calling a fraudulent tech support number.

Once on the phone, the scammer may ask you to grant remote access to your computer so they can "fix" the problem. In reality, they're installing malware or stealing sensitive information. In some cases, they'll even demand payment for bogus security software that does nothing.

How to Protect Yourself

- If you see a pop-up like this, do not call the number—simply close your browser and restart your computer.
- Never allow remote access to your computer unless you're working with a verified IT professional.
- Keep your device updated with trusted antivirus software to block real threats.

Scam Texts About Unpaid Tolls

You're sitting at lunch when a text pops up—**"**FINAL NOTICE: You have an unpaid toll balance. Pay now to avoid late fees." It includes a link, and for a moment, you wonder: *Did I forget to pay a toll?*

Scammers hope you won't stop to think. Clicking the link takes you to a fake payment page that looks identical to an official toll agency website. Once you enter your credit card information, they've got what they need to steal your money or commit identity theft.

How to Protect Yourself

- Do not click links in unexpected text messages about unpaid tolls. Instead, visit the state's official toll website to check your account.
- If you're unsure, call the toll authority directly using a verified phone number.

- Watch for urgent language in messages—legitimate toll agencies don't send threatening texts demanding immediate payment.

Stay One Step Ahead of Scammers

Scammers succeed because they create a sense of urgency, making people act before thinking. The best way to protect yourself is to slow down and verify before engaging. If you ever receive a suspicious pop-up, text, or phone call, ask yourself:

- Is this unexpected? Legitimate companies don't contact customers this way.
- Am I being pressured? Scammers want quick action before you can double-check.
- Can I verify this information? Always go directly to the source, whether it's Microsoft, a toll agency, or your bank.

Falling for a scam doesn't mean you weren't paying attention—today's fraudsters are incredibly convincing. But the good news is, you have the power to stop them in their tracks**.** By staying informed, questioning unexpected messages, and resisting pressure to act quickly, you can avoid becoming a target. The next time a pop-up warns of a virus or a text demands an urgent payment, take a breath, step back, and verify. Scammers rely on fear and urgency, but a moment of caution is all it takes to protect yourself and your finances. Stay aware, trust your instincts, and when in doubt—don't engage.