



New Scam Tactics for 2024

Cybercriminals leverage emerging technologies and exploit human psychology to devise new methods for deception, fraud, and data theft. Understanding these evolving tactics is crucial for safeguarding personal information and financial resources in the coming year.



Stay Alert and Aware

AI-Generated Personalized Scams

Scammers are now utilizing AI algorithms to analyze vast amounts of data from social media profiles, public records, and other online sources. This enables them to craft messages that appear from trusted sources or that reference specific personal details, making them more convincing and challenging to detect.

Student Loan Forgiveness Scams

These fraudsters often pose as representatives of legitimate loan forgiveness programs or government agencies, offering false promises of reducing or eliminating student debt in exchange for an upfront fee or personal information. Borrowers must verify any loan forgiveness offer through official government channels and be skeptical of any scheme that demands immediate payment or sensitive information.

Text Message Scams

Scammers send fraudulent text messages to trick recipients into providing personal information, clicking on malicious links, or downloading harmful software. These messages often appear to come from legitimate sources such as banks, delivery services, or government agencies and may include urgent language to prompt immediate action.

Phone Scams

Don't get flustered if you receive a call that seems serious out of the blue. Instead, ask for a case number and then hang up. After that, contact the organization using official contact information to verify the call's legitimacy. This practice ensures that you speak with a genuine representative and helps protect you from falling victim to these fraudulent schemes.

If you receive an unexpected email, text message, or phone call, you need to figure out if it's real or a scam and report it to the **IT Help Desk** before taking any action. Remember, there is nothing urgent about unsolicited communications, so take the time to verify their authenticity. The **IT Help Desk** is there to assist you, offering guidance on managing such situations safely. By taking these precautionary steps, you ensure your protection against potential scams and safeguard you and your organization's information.