Navigating the Digital Landscape: Staying Safe from Scams in the age of AI

In this presentation, we'll look at scams in the digital world, which have been supercharged in the last year thanks to AI. We'll equip your knowledge toolbox with tips to identify and avoid the latest scams.

Together, let's empower you to use technology with confidence and peace of mind!

by Lökwest Consulting

Understanding the Evolving Threat Landscape

Let's take a look back at three ways you're likely to get scammed. The first step in identifying scams is to determine their **TTP's** or "techniques, tactics, and procedures." In other words, how did they get in, what do they want, and what does it mean for you?

Outdated Software

Keeping your devices updated is crucial to prevent hackers from exploiting vulnerabilities, just like regular car maintenance.

Data Breaches

A data breach is like leaving your house keys in the door - your personal information can be stolen and misused.

Targeted Attacks

Scammers tailor their attacks, like a thief picking a specific target. Be vigilant for signs of phishing or scam calls.

Consequences

These threats can lead to financial loss, identity theft, and emotional distress. Understanding the risks helps us stay proactive.

The Influence of Social Media and Algorithms

Manipulative Algorithms

Social media platforms may use algorithms to subtly shape your views and feed you misleading information without your knowledge.

- **Search Results Misdirection**: Algorithms prioritize "free" offers leading to scams.
- **Misleading Customer Support Numbers**: Promotes fake service numbers, connecting users with scammers.
- **Targeted False Ads**: Targets users with ads making unverified claims, exploiting trust.

The Influence of Social Media and Algorithms

Zombie Internet

Real interactions are being replaced by automated scripts and bots, cluttering your feeds with false and misleading content.

- **Automated Fake Interactions**: Social feeds filled with bot-generated comments and likes, diluting genuine engagement.
- **Misleading Content Spread**: Bots and scripts rapidly spread false information, overshadowing real news and discussions.
- **User Manipulation**: AI-curated content manipulates opinions by selectively showing or hiding posts, shaping public perception without transparency.

The Influence of Social Media and Algorithms

Algorithm Driven Echo Chamgers

Social media algorithms can create echo chambers that reinforce users' existing beliefs by selectively showing content that agrees with their views, limiting exposure to diverse perspectives.

- **Reinforcement of Beliefs**: Users see more of what they agree with, lessening exposure to opposing views.
- **Isolation from Diversity**: Algorithms filter out diverse opinions, fostering a narrower worldview.
- **Polarization of Discussions**: Intense focus on preferred topics intensifies opinions, reducing balanced discussions.

Scams Evolve: The Man in the Middle

1

Fake Notifications

Scammers may send convincing-looking messages, like a fake banking app alert, to trick you into revealing sensitive information.

2

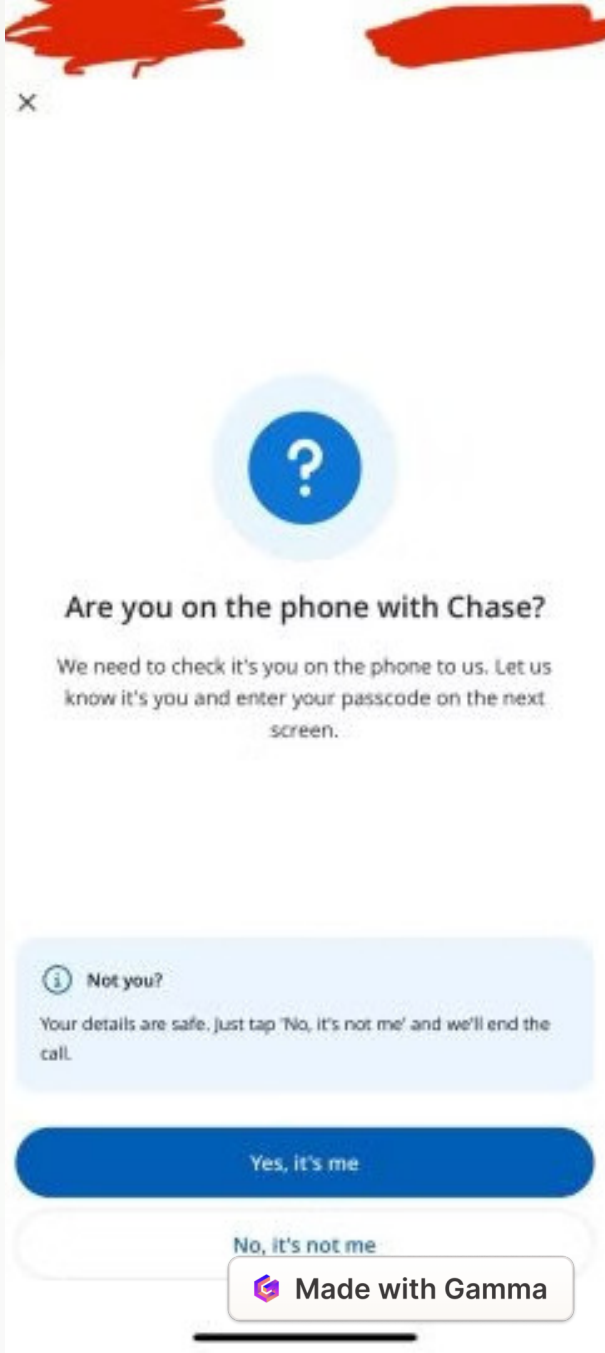
Verify Through Trusted Channels

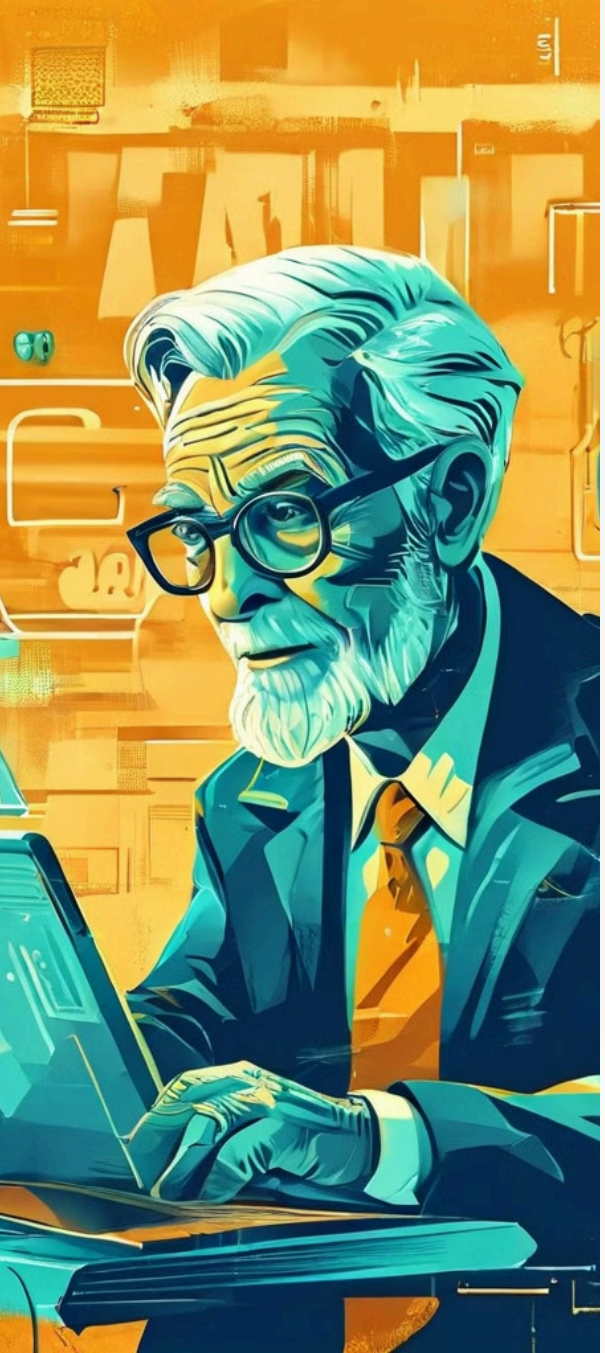
If you receive a suspicious message, contact your bank directly using a number you know is safe, not one provided in the message.

3

Stay Vigilant

Remain cautious of any unexpected digital requests, even if they appear to be from a legitimate source.





Scams Evolve: AI-Cloned Voices

YouTube

LKW as ai

Scams Evolve: AI-Cloned Voices

1. Remember that AI-generated audio is becoming increasingly **difficult to detect**. Scammers can now replicate human voices with near-perfection.
2. Always **hang up and call back** using a known, trusted number when receiving unexpected requests for money or personal information.
3. Agree on a **secret safe word** with loved ones in advance, to verify identity in an emergency.
4. Ask a **personal question** that only the real person would know the answer to, like "What did we have for dinner last night?"
5. Understand that **any voice**, even your own, can be **mimicked** using AI tools with just a few seconds of audio.
6. Be wary of **emotional appeals** that try to create a sense of urgency - take a moment to reflect before acting.

Scams Evolve: Spotting the Bots

1 AI-Generated Messages

Scammers use AI to create more believable phishing emails and fake profiles, making them harder to detect.

- Check for Odd Phrasing
- Verify Unexpected Contacts
- Check the return address
- Look for Consistency

2 AI-Generated Imagery

Scammers use AI to create more realistic images and videos, enhancing the credibility of fake profiles and fraudulent schemes.

- Inspect for Irregularities
- Cross-Verify Images (Google image search)
- Evaluate Context Relevance

3 Flattering or Urgent Requests

Be critical of messages that seem too good to be true or pressure you to act quickly.

- Immediate Payment Demands
- Fast Action Bonuses
- Security Alerts

4 Inauthentic Communication

Trust your instincts - if something feels off, it's better to err on the side of caution.

- Verify Directly
- Pause and Reflect
- Consult Trusted Sources

Protecting Yourself with Best Practices

Strong Passwords

Use unique, complex passwords for each of your accounts.

Two-Factor Authentication

Enable this extra layer of security to protect your accounts.

Regular Software Updates

Keep your devices and software up to date to patch vulnerabilities.

Protect Yourself with Knowledge

1

Understand the Risks

Learning about digital threats helps you use technology safely.

https://www.snopes.com/

https://consumer.ftc.gov/

https://www.security.org/

2

Stay Informed

Regularly check reputable sources for the latest security updates.

Our newsletter is a great monthly roundup of technology news!

read.lokwest.com

3

Continuous Learning

Maintain your digital literacy to navigate the evolving landscape.

https://www.digitallearn.org/

https://seniorplanet.org/

https://techboomers.com/

Let's Talk - Q&A and Resources

Questions?	Unmute to ask or type in the chat now!
Experiences to Share?	We'd love to hear about your personal encounters with digital threats.
Get in Touch	Visit us at: https://lokwest.com Bookings: https://bookings.lokwest.com Phone: 949.388.0241 E-mail: info@lokwest.com