Emerging DNS Abuse Trends video

Executive Summary: The State of Internet Safety

The text is a transcript from a 2026 webinar featuring experts from **ICANN** (the organization that coordinates the internet's "phone book") and industry leaders. They discuss how internet criminals are using new technology—especially **Artificial Intelligence (AI)**—to launch attacks faster than ever before, and how the "good guys" are fighting back with automation.

---

1. The "Iceberg" Problem: Scams are Exploding

The experts highlight that what we see online is just the "tip of the iceberg." Most scams go unreported.

- **The Trend:** In 2025, over **100 million** new website names (domains) were created. About **25%** of them were suspicious or malicious.
- **Constant Attacks:** Phishing (fake emails or texts) used to happen in waves, like during tax season. Now, it is a "sustained barrage." The average user is protected from about **66 threats every single day**.
- **The AI Factory:** AI has made it incredibly cheap and easy for criminals to create harmful content. For example, AI-generated child abuse material saw a staggering **26,000% increase** because the software can now create fake videos in seconds.

  Layman Example: Imagine a criminal who can build 1,000 fake storefronts in an hour. By the time the police shut one down, the criminal has already moved to ten others. This is called "high churn."

---

2. How the Attacks Happen

Cybercriminals don't just use email anymore. They are moving to where you spend your time.

Method	How it works	Percentage
Phishing	Fake messages via WhatsApp, SMS, or Facebook Messenger.	**60%**
Vulnerability	Exploiting a "hole" or "weakness" in your phone or computer software.	**21%**
Other	Various technical hacks or malware.	**19%**

---

3. The New Defense: "Digital Shield" Strategies

To keep up with fast-moving criminals, the experts are moving away from manual human reviews to **automated systems.**

- **From Days to Seconds:** In the past, it took about **96 hours** (4 days) to take down a bad website. New automated systems can now do it in **seconds**.
- **The "Sinkhole" Strategy:** Instead of just deleting a bad website, experts "sinkhole" it. They redirect the traffic to a safe server so they can study the criminals' patterns and see who else they are trying to trick.
- **Campaign Spotting:** Instead of playing "Whac-A-Mole" with one website at a time, defenders now look for "campaigns"—large batches of thousands of websites registered at the same time by the same person.

---

4. Global Rules and Cooperation

The **UK’s Online Safety Act (2025)** is now in full force, requiring internet companies to take more responsibility for child safety and illegal content. The experts emphasize that because the internet has no borders, companies (ISPs, registrars, and tech firms) must share data instantly to stop scams before they reach your phone.

Main Takeaway for You

The internet is currently facing a "volume explosion" of scams powered by AI. While the industry is building faster, automated shields to protect you, **personal vigilance is more important than ever** because criminals are constantly changing their "masks."

Would you like me to create a simplified checklist based on this info to help you identify these "Emerging DNS Trends" in your own inbox?