IDENTITY THEFT TODAY

Device Takeover: When Criminals Hijack Your Tech

June 17, 2026
12pm - 1pm EST

LEGAL RESOURCES

SESSION NOTES

Below is a summary of the topics and items discussed in the June 2026 session of **Identity Theft Today: Device Takeover: When Criminals Hijack Your Tech.**

SESSION TOPICS

What Is Takeover | Devices at Risk | How It Happens | Malware Types | Warning Signs
Free Protections | Paid Protections | Public Wi-Fi Risks | Smart Home Security

Click Here to Access Recorded Session ⟶

WHAT TAKEOVER MEANS

- Distinct from simple account access — the attacker can see, change, and act as you acrosseverything the device touches.
- Not isolated to one username/password; it's control of the whole device and every app logged into it.
- Analogy: a thief steals your house keys and installs hidden cameras — they no longer need to break in.

DEVICES AT RISK

- Obvious targets: smartphones, laptops, tablets.
- Less obvious: smart-home gear (Ring doorbells, garage openers, thermostats), smart TVs, and voice assistants — all are connected computers.
- Rule of thumb: anything internet-connected with access to something you value is a potential target.

HOW TAKEOVERS HAPPEN

- Malicious apps/games carrying malware; phishing links via email or text; weak or reused passwords; unsafe public Wi-Fi; unsafe downloads.
- The recurring theme: "the bad guys don't hack in — they log in" using easily guessed or reused credentials.
- Most are crimes of opportunity (a broad net), not targeted attacks.

MALWARE'S ROLE

- Designed to spy (collect and report info) or control, directed through a command-and-control channel.

- Variants: spyware, keyloggers (capture every keystroke), and remote-access tools (let an attacker operate the device remotely).

A REAL CASE

- April 2026 SOHO router compromise leading to DNS hijacking — a foreign state-nation actor took over tens of thousands of home routers, later weaponized for DDoS activity.
- Brian's own example: a "threat detected" alert from his smart router flagging reconnaissance against his Skybell door camera, traced to a cloud-hosted IP — a reminder to enable router alerts and investigate them.

WARNING SIGNS

- Six signals: fast battery drain, overheating, unexpected pop-ups, unknown login locations, randomly changing internet speeds, plus smart-home oddities (cameras recording unprompted, doors unlocking, doorbells triggering, assistants talking back).
- Any one alone is explainable; two or three recurring together warrant investigation.

PROTECTIVE HABITS

- **No cost**: keep devices and apps updated, use strong unique passwords, enable MFA/2FA, install only trusted apps with necessary permissions, and avoid suspicious links — "verify before you trust."
- **Some cost**: turn on built-in device security, use a password manager, add security/antivirus software, and upgrade aging routers to ones with network-protection controls.

KEY TAKEAWAYS

- Your device is your digital front door — keep it locked.
- Small, consistent habits matter as much as the technology.
- The human-behavior element is as important as any technical control.

Q&A HIGHLIGHTS

Q1. Can someone access my phone just by being nearby if they have my number?

A: Can someone access my phone just by being nearby if they have my number?
Certain features can expose you in close proximity — AirDrop is one, and Bluetooth is another (more sophisticated) vector. Best practice: turn off Bluetooth, Wi-Fi, and AirDrop when you're out in public or traveling.

Q2. I'm getting a flood of scam-likely calls — how do I stop them?

A: Start with your carrier (Verizon, T-Mobile, etc.) — they can apply controls you can't access yourself and advise on handset settings like reporting or rejecting unknown callers.

Q3. Can you recommend a smart router?

A: Brian personally uses Ubiquiti — positioned between consumer and business grade, with solid support and value (no affiliation). The key feature to look for is built-in threat alerting.
, confirm all software updates are applied first, then follow the same approach.

Q4. My iPhone has excessive battery drain and my MacBook camera turns on by itself — how do I know if it's a takeover?

A: Back up the phone, do a factory reset, then restore. If the behavior continues, do a factory reset withoutrestoring from backup (to avoid reapplying anything malicious). For the MacBook

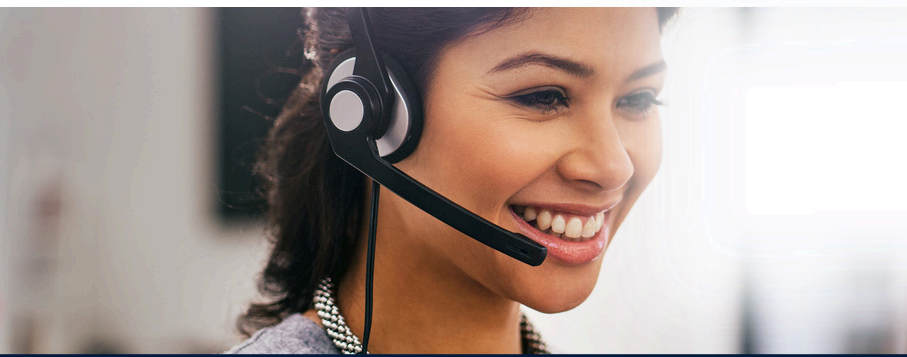
Q5. Can my credentials be stolen on public Wi-Fi if I only use saved logins?

A: Yes, it's possible if someone is capturing traffic and the exchange happens in clear text. Saved logins, passkeys, and MFA reduce the risk — but on any public network, use a VPN, which encrypts your traffic through a secure tunnel.

ABOUT THE SPEAKER:

BRIAN BROTSCHI | ROSE ADVISORY BOARD MEMBER

Brian Brotschi is an advisory board member of ROSE (Resources Outreach to Safeguard the Elderly), an organization dedicated to protecting older adults from cybercrime and scams. A longtime IT and security professional, he currently works at Microsoft Corporation, focused on protecting large enterprises from cyber threats.



Contact Us

Our Member Services team is available for assistance.

Phone: 800.728.5768
Email: info@legalresources.com

www.legalresources.com