YOUR ROUTER CAN PUT YOUR ACCOUNT AT RISK

Lessons from the Forest Blizzard / APT28 Router Exploitation Case

Router security = account security

1. What happened?

- Since at least August 2025, Forest Blizzard/APT28 exploited vulnerable SOHO routers.
- They changed router DNS settings rather than hacking each user's computer.
- Selected login and email traffic could be redirected.
- Attackers aimed to steal passwords, tokens, and other credentials.

Why this matters

The attack may allow adversary-in-the-middle (AitM) theft of credentials or tokens, even after MFA.

2. Attack mechanism

1. **Compromise router** — Exploit an unsupported or vulnerable SOHO router.
2. **Change DNS settings** — DNS requests are sent to an attacker-controlled resolver.
3. **Stay quiet** — Most requests still return legitimate IP addresses.
4. **Redirect selected requests** — Email, cloud, or login traffic is redirected.
5. **Steal credentials / tokens** — Passwords, MFA codes, or session tokens may be captured.

What is DNS?

DNS is like the internet's address book.

3. User-level defenses

A. Do not ignore TLS warnings

Close the page and try again from a trusted network. Never enter passwords or MFA codes after a TLS warning.

TLS helps confirm that you are connecting to the real website, not an imposter.

B. Maintain the router

- Replace end-of-life routers
- Update router firmware
- Enable automatic updates
- Check DNS settings: use ISP DNS or another trusted resolver

Because ordinary users may miss these steps, router security also raises broader policy questions.

4. Policy questions and suggestions

A. Vendor responsibility

- Disclose support periods
- Provide security updates during that period
- Warn users when support ends
- Consider minimum support periods and automatic updates

B. ISP responsibility

- Notify customers when routers appear to use suspicious DNS resolvers
- Help users remediate the problem
- Reserve blocking for clear, serious cases
- Balance security with privacy and overblocking concerns

Conclusion

The Forest Blizzard/APT28 case shows that account security depends not only on passwords or MFA, but also on router security.

★ ★ ★ **Key takeaway: Router security is account security.** ★ ★ ★