Fake Sites, Real Danger: Understanding Typosquatting

What Is It?

Typosquatting occurs when cybercriminals register fake website addresses that look almost identical to popular sites, hoping you'll make a typing error and land on their page instead.

Common Examples

- Replacing the "o" with a "0"
- Omitting or adding additional letters
- Replacing letters with numbers
- Changing the domain (e.g., from .com to .net)

Why Do They Do This?

Typosquatters want to:

- **Steal your information** (e.g., passwords, credit cards)
- **Install malware** on your device
- **Make money from ads** you accidentally view
- **Trick you** into buying fake products

How To Stay Safe

Check the URL carefully before entering any information

Use bookmarks for sites you visit frequently

Look for HTTPS and the padlock or "tune" icon in your browser for a secure connection

Enable browser warnings for suspicious sites

Use password managers that only auto-fill on legitimate sites

Use Multi-Factor Authentication (MFA), requiring two or more proofs of identity to protect against unauthorized access

Remember

One small typo can lead to big problems. When in doubt, close the page and retype the address carefully or search for the official site through a trusted search engine.