Skillmine
Technology • Consulting • Services

Brand Impersonation:
Trust Is the Target

What Is Brand Impersonation?

Brand impersonation is a technique where attackers misuse trusted platforms, services, or familiar branding to make malicious content appear legitimate.
Instead of creating obviously fake websites, attackers often use real platforms or convincing replicas to deliver deceptive login pages that appear safe and trustworthy.

Why It Works:

- Familiar platforms reduce suspicion
- Trusted domains appear legitimate
- Login pages closely resemble official services
- User trust lowers caution

How the Attack Happens

- A malicious link is shared using a trusted-looking service or platform
- The page imitates a legitimate login or verification screen
- The user enters credentials or sensitive information
- The attacker captures and misuses the information

Potential Impact

- Account compromise
- Unauthorized access
- Data exposure
- Business email misuse

Where These Attacks Commonly Appear

- Shared cloud documents
- Login or verification pages
- File access requests
- Collaboration or messaging tools
- Email notifications claiming urgent action

Pause and Verify

Before entering credentials or approving requests, ask yourself

- Is this request expected?
- Does the page behave normally?
- Was the link accessed through an official or trusted path?
- Am I being asked to act urgently or unexpectedly?

Real-World Examples

Microsoft has warned about phishing campaigns where attackers abused services such as SharePoint and OneDrive to distribute links leading to fake login pages designed to mimic official Microsoft sign-in portals.

How to Stay Safe

- Use official websites or bookmarks to sign in
- Avoid entering credentials through shared links
- Verify unexpected requests independently
- Focus on behavior and context, not just appearance
- Report suspicious links or login pages to the IT/Security team

Key Message

Brand impersonation attacks exploit trust, not just technology.
If something looks familiar, verify it before you trust it.