SECURITY INSIGHTS:

Phishing kits are reaching the enterprise level

Genady Vishnevetsky, Chief Info Security Officer, Stewart Title Guaranty Company

Remember when we used to spot phishing emails by their broken English and urgent requests from a "Nigerian prince"? Those days are long gone. Today's cybercriminals are running their operations like Fortune 500 companies, complete with professional-grade software, customer support, and even subscription models. The latest example is a phishing kit called **Salty2FA**, which is making two-factor authentication look about as secure as a screen door on a submarine.

Think of Salty2FA as the Netflix of phishing attacks. For a monthly fee, any wannabe hacker can rent this sophisticated toolkit that does all the heavy lifting. They don't need to know how to code or understand complex security systems. The kit comes ready to deploy, like ordering takeout instead of cooking from scratch. What makes this particularly unsettling is that it defeats the very security measure we've been told would keep us safe: two-factor authentication.

Here's how it works. Target receives an email that appears to be from their company's IT department or a trusted business partner. The email may mention an urgent document to review or a billing issue that needs to be resolved. When the user clicks the link, they are taken to a page that resembles their company's login portal, complete with the same colors, logo, and other elements. Even the web address looks convincing. When the target enters their credentials and that two-factor code arrives on their phone, the phishing page captures it in real-time. The attackers use automation to immediately log into the victim's real account with both their password and the fresh authentication code. By the time the victim realizes something's wrong, they're already inside the target's account. The kit can intercept SMS codes, authenticator app codes, and even push notifications – essentially every common form of two-factor authentication except hardware keys.

What makes this especially clever is how the kit hides in plain sight. It uses legitimate platforms and creates a new web address for each victim, making it nearly impossible for security teams to block. It's like a criminal using a different fake ID for every person they meet - by the time one is flagged, they've already moved on to the next.

The kit even customizes itself automatically. It instantly creates a fake login page with the target company's branding. This group looks up the domain associated with the victim's email address (i.e., Joe.Smith@titlecompany.com) and automatically pulls logos, styles, templates, and graphics from a legitimate website. Then, it dynamically populates the phishing landing site to make a replica.

TAKEAWAYS:

1. **Pay attention to the URL** in your browser's address bar. Even sophisticated phishing sites often have subtle differences – an extra dash, a different domain extension, or an unfamiliar subdomain. If you're logging into Microsoft 365, the address should start with **login.microsoftonline.com**, not something similar-looking

2. When you receive an **unexpected login request via email**, navigate to the site manually instead of clicking the link. Open a new browser tab and type the address yourself, or use a bookmark you've previously saved

3. **Consider implementing hardware security keys** for critical accounts to enhance security. Unlike phone-based codes, these physical devices use cryptographic verification that can't be intercepted or replayed by phishing sites

4. **Trust your instincts.** If something feels off about a login page-maybe the logo looks slightly fuzzy or the page loads in an unusual way-stop and verify through an alternative channel. Call the sender using a phone number you already have, not one from the email

The reality is that two-factor authentication remains valuable – it effectively stops many automated attacks. But it's not bulletproof. As these phishing kits become increasingly sophisticated and accessible, we must adjust our security mindset accordingly. It's no longer enough to enable two-factor authentication and assume we're protected.