FMBusinessDaily

New data highlights UK cybersecurity gap with MFA bypassing phishing attacks increasing

10 months ago

Recently, there has been an increase in phishing email attacks that are designed to bypass multi-factor authentication (MFA), leaving businesses across the UK vulnerable.

New survey data released this October Cyber Security Month by cyber experts at the NEBRC has found that over half of UK workers (54%) have experienced some form of phishing incident within their work environment. Only 35% of workers claim that nothing has ever happened to them or someone they know regarding phishing emails and 11% weren't sure if anything had happened.

The research conducted with 1,000 British working adults found a gap in workplace protection, with limited and outdated training. Over half (53%) have had no training, can't remember any training or have outdated training in MFA and phishing.

So, what Are MFA Bypass Phishing Email Attacks?

Phishing emails are deceptive messages sent by hackers pretending to be legitimate contacts or organisations. These emails aim to trick recipients into one of three things:

- Clicking on a malicious link
- Opening a dangerous attachment
- Divulging sensitive information, such as passwords, or making fraudulent payments

Martin Wilson, Police Detective Inspector and Head of Student Services at NEBRC (North East Business

Resilience Centre) explains,

"The latest trend in phishing involves hackers using compromised, legitimate email accounts to send these phishing emails. Instead of creating fake email accounts that are easy to spot (like "ebbay.com" instead of "ebay.com"), hackers prefer to take over real accounts and send malicious emails to people in the victim's address book."

How Hackers Bypass MFA

Martin adds,

"Typically, a phishing email prompts the recipient to open a link or attachment, which leads to a fake login page (like a fake Microsoft 365 sign-in page). The page requests the user's login credentials, and if the user provides them, the hacker captures the username and password.

If the compromised account has MFA enabled, you have an additional layer of protection. However, certain types of MFA, like SMS text codes or authenticator apps, can still be bypassed."

Here's how:

- OTP (One-Time Password) Interception: When you enter the MFA code (sent via SMS or generated by an authenticator app), the hacker can steal it in real-time. They then use the code to gain access to your account.

Once inside, hackers often:

- Send phishing emails to your contacts, rapidly spreading the attack.
- Set up email rules that hide incoming messages from your inbox, making it harder for you to notice the compromise.
- Continue using the account until someone, usually a recipient of a suspicious email, contacts the account owner to alert them of the issue.

Why SMS or Authenticator App MFA Can Be Vulnerable

MFA methods that rely on SMS or authenticator apps are vulnerable for a few key reasons:

1. SIM Swapping (for SMS): Hackers can trick your phone carrier into transferring your phone number to their device, allowing them to receive the OTP code and access your account.
2. Phishing (for SMS and Authenticator Apps): Hackers can create fake login pages that look legitimate. You enter your username, password, and the MFA code, which the hacker then captures and uses to log in themselves.
3. Malware: If your device is infected with malware, the hacker can intercept the MFA code as you enter it.

More Secure MFA Methods: On-Screen Codes and Physical MFA Keys

To mitigate these risks, consider using more secure forms of MFA, such as:

- On-Screen Codes: Some MFA systems display a code on your screen, which you verify with an app or

physical device instead of typing it in. This can make it harder for hackers to bypass MFA during a phishing attack.
- Physical MFA Keys: Devices like USB security keys are extremely hard to compromise. A hacker would need to physically possess the key to log in, making phishing attacks ineffective.

Why These Methods Are More Secure

- No Typing Required: You don't have to manually enter a code, so hackers have nothing to intercept.
- Challenge-Response System: With a physical key, the authentication process happens securely between the device and the system, without exposing any sensitive information.
- Harder to Fake: Physical keys and app-based verifications like push notifications require direct user interaction, making it much more difficult for hackers to trick you.

Over one in five (22%) of workers don't use any type of MFA in their workplaces. The most common types of MFA protection experienced by workers are,

- 21% (over one in five) use time-based, one-time password/code within an App
- 20% (a fifth) use time-based, one-time password/code via SMS
- 20% (a fifth) use time-based, one-time password/code via email
- 17% (over one in six) use pre-set security questions
- 17% (over one in six) use biometric authentication
- 12% (one in eight) weren't sure
- 9% (less than one in ten) use physical MFA keys such as a key or fob

Avoiding MFA Fatigue Attacks

While using an app-based MFA is generally secure, you should be cautious of "MFA fatigue" attacks. In this scenario, hackers send many login requests to the victim's phone, hoping they get frustrated and approve one of them just to stop the notifications. Always be mindful of login attempts you didn't initiate, and never approve a request unless you're certain it's legitimate.

Steps to Protect Your Business from MFA Bypass Attacks

1. Educate Your Team: Ensure employees know how to spot phishing emails and understand the risks of opening suspicious links or attachments.
2. Implement Stronger MFA: Use MFA methods that rely on physical keys or app-based verifications rather than SMS or codes.
3. Be Cautious of Unusual Activity: If you notice unexpected login attempts or MFA prompts, investigate them immediately.
4. Regularly Review Email Rules: Check your email settings for suspicious rules that could hide important messages from your inbox.
5. Use Spam Filters: Ensure your business has up-to-date spam filters that can detect phishing attempts.
6. Set up Geolocation Rules: Consider only allowing MFA requests from UK-based requests, denying requests that don't originate in the UK – sometimes technical controls can be brought into play to achieve this.

Outdated training

Shockingly, almost a third of workers (32%) have never undertaken training on phishing attacks or MFA. A further 6% (almost one in sixteen) haven't had training within the last year and 15% can't remember when they last had this training, if ever. Which may signal that any training they did receive wasn't engaging or memorable.

What's more surprising is that 66% (two-thirds) of business owners haven't had training on MFA or phishing within the last year, with a shocking 50% saying that they have never undertaken training in this area. This is surprising given, the huge financial and reputational damage such breaches can cause.

The NEBRC can provide training that can help business owners articulate and comprehend these risks to their employees and a network of partners that can implement spam filters and help you choose the right MFA for your business. Additionally the National Cyber Security Centre (NCSC) has some great guidance and further resources on MFA and phishing.