THEFRAUDPRACTICE
PROTECTING THE BOTTOMLINE

THERE IS NO SILVER BULLET:
USER CREDENTIALS ARE NOT SECURED WITH 2FA ALONE

White paper presented by The Fraud Practice

THERE IS NO SILVER BULLET: USER CREDENTIALS ARE NOT SECURED WITH 2FA ALONE

By: Lawrence Baldwin and Justin McDonald

A white paper by The Fraud Practice and myNetWatchman

Sponsored by myNetWatchman

2FA Myths and Misconceptions

Many argue that implementing two factor authentication (2FA) comprehensively across all user applications is not only a good idea, but an obvious imperative that ultimately solves many account security woes. Unfortunately, the reality is that opting for 2FA is a complex decision that is certainly appropriate and critical in some scenarios, but in others is overly costly, high friction, impractical and, in some cases, can cause more harm than good. Similarly, there is often an implication that the existence of a second factor is a cure-all enabling you to safely ignore known vulnerabilities in the first factor (traditional username/ passwords). Lastly, some assumptions regarding the benefits of 2FA were originally valid but are now significantly weaker because the threat actors have deployed new tools and tactics that make 2FA vulnerable. First, let's dispel three common misconceptions about 2FA.

Consumers tend to reuse passwords, even with email and mobile phone accounts, meaning 2FA can be beaten with SIM swap scams and email account takeover.

Consumers are Okay with 2FA

2FA may be expected and tolerated with online banking, financial services and other accounts with sensitive information or access to monetary value behind the account, but this is not the case for most industries. For eCommerce retail especially, 2FA is at most something organizations can offer but not require, and most customers will choose not to opt-in. Most risk teams have to be conscious about friction and 2FA is a significant factor in inhibiting user experience (UX). A recent survey from NordPass[1] found that the average number of passwords a consumer has for personal use is now 168 in 2024, up from 80 at the start 2020. It is unrealistic to expect consumers to accept 2FA across all of their accounts while consumers are becoming increasingly more annoyed with, and therefore less likely to opt-in to using, 2FA as the number of accounts and passwords they have continues to rise.

> "The average consumer has over 150 online accounts protected by a password while using 47 different mobile apps at least once per month on average.[2] 2FA will not scale to be used by a consumer as a standard process across all of these interactions."
>
> **David Montague**
> **CEO, myNetWatchman**

2FA Means User Accounts are Fully Secure

There are two primary reasons why this is not the case. First and most impactful is that 2FA can be beaten. Account takeover (ATO) of an email address can accompany the ATO attempt an organization is seeing, meaning the attacker has access to the one-time passcode (OTP) sent via email. Ways to beat 2FA are only getting more sophisticated with SIM swap (ATO of a phone number) attacks and other means. Second, is that presenting 2FA validates to the bad actor that the username and password combination they presented is a working credential, otherwise they would not have been prompted to complete 2FA. Often, just this validation of the active credential pair is all the attacker is after.

Sources:

1 - https://nordpass.com/blog/how-many-passwords-does-average-person-have/

2 - https://sensortower.com/blog/number-of-apps-used-per-device-2021

Credential Stuffing Attacks Will Stop if you Implement 2FA

> "Companies often believe focusing on 2FA is the first order of business when they are seeing a lot of ATO, but they shouldn't be thinking about 2FA until they resolve the first factor problem of reuse and bad passwords."
>
> **Lawrence Baldwin**
> **Founder, myNetWatchman**

2FA does nothing to protect the first factor: the password. As prefaced above, presenting 2FA after a login attempt validates that the username or email address being presented has an active account and that the password used with it is still currently in use. While 2FA can protect access to monetary value and the personally identifiable information (PII) that is associated with the user account by not allowing access to it, it doesn't eliminate the value credential stuffing attacks add to credentials compromised elsewhere. Email and password harvesting is a common tactic causing more issues for the users down the road with targeted phishing campaigns and other attacks that will be associated with brand risk. In short, organizations still need to be focused on detecting credential stuffing attacks and on securing account credentials as a precursor to presenting 2FA.

For the purposes of this white paper, let's focus on the considerations for 2FA in a single, specific use case: consumer eCommerce, or what may also be referred to as Business to Consumer (B2C) eCommerce. Here are the key factors related to this use case:

- **Merchants often have a very large user base (potentially tens of millions)**
- **The user base is not security conscious**
- **Users are highly sensitivity to added friction**
- **The average user practices poor password hygiene (weak and/or breached passwords are frequently used)**
- **The financial loss per fraud event is relatively low (few hundred dollars per event)**
- **Aggregated losses from fraud can be substantial due to the size of the user base**
- **Merchants hold the liability for losses**

With or without 2FA, organizations must still protect the first factor: the password.

Next, let's examine the common and major threats leading to account compromises and the effectiveness of 2FA in combating each. This includes:

- **Credential Stuffing**
- **Traditional (bulk) Phishing**
- **Advanced (targeted reverse-proxy) phishing**
- **Malware (keystroke loggers/info stealers)**

Effectiveness of 2FA with Common Account Compromise Attacks

Credential Stuffing

Daily, myNetWatchman observes over 50 million credential stuffing login attempts against tens of thousands of targeted organizations.

A common assertion is that 2FA "stops 99.99% of credential stuffing attacks." This is extremely short-sighted and misleading. It is true that deploying 2FA will effectively prevent a credential stuffing attack from fully authenticating into an account, however, it absolutely does not mean the attack is neutralized.

At myNetWatchman, we have a unique perspective on credential stuffing as we directly observe over 50 million credential stuffing authentication attempts against tens of thousands of targeted organizations every day. When a malicious actor tests a credential pair against a 2FA enabled website and the credential pair is valid, the website logic typically sends a referral to a 2FA challenge page. The actor can't proceed further if they have not also compromised the second factor, however, they have already obtained extremely valuable information:

"Across myNetWatchman data, we see bad actor credential stuffing attacks where they are harvesting on sites to see where they get prompted for 2FA and thus know a username and password combination is being used and is valid there."

Rob Long
CTO, myNetWatchman

1. **The username/email address that was validated is confirmed as an active customer of the tested website**

2. **The username/password pair is valid**

This is known as email or email and password harvesting. The actor has harvested a list of email addresses with an associated compromised password that they have validated to be in use at a given merchant or organization. The attacker can then use the output of this attack to develop a curated list of confirmed customers to feed a highly targeted advanced phishing attack against those victims. Alternatively, they can just package this higher quality information for resale to other bad actors who will do the same.

So 2FA does not really neutralize the overall account compromise threat, rather it prevents accounts from being directly compromised through credential stuffing and forces the bad actors to do a bit more work to ultimately accomplish their objective.

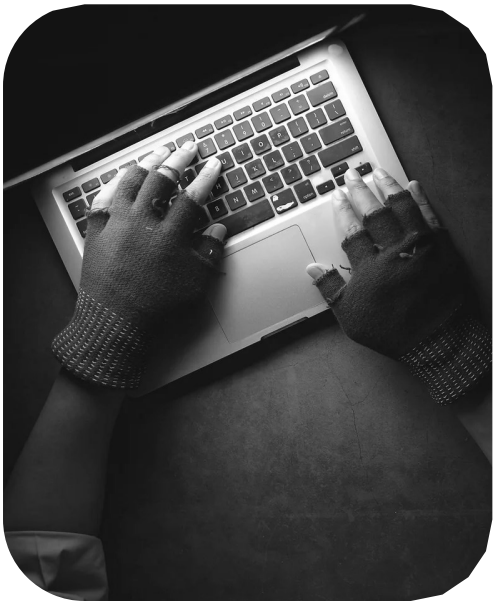
Traditional Phishing

With traditional phishing, attackers are typically sending out email or SMS messages attempting to trick prospective victims into entering their usernames and passwords into a fake login page. The impact of 2FA on simple phishing is much like its impact on credential stuffing. Attackers won't be able to fully authenticate with usernames and passwords alone. They could attempt to also phish the second factor, but since 2FA codes are typically invalidated after a relatively short time frame (e.g. 30 seconds), it is fairly difficult for the attackers to act on this information before it times out.

Due to the widespread consumer reuse of passwords, credentials compromised from phishing attacks targeting other organizations can be used against many more targets in the future.

Additionally, some types of 2FA mechanisms (e.g. push notifications, U2F) can't be phished as they involve the end-user performing an action (e.g. clicking OK or pushing a physical button). However, as with credential stuffing, 2FA fails to prevent simple phishing attackers from obtaining valuable information, namely valid credentials and likely confirmation that a given victim is a confirmed customer of the organization targeted by the phishing attack. In other words, if the attacker is trying to harvest a list of emails associated with a user account, they have accomplished their goal.

Keystroke Loggers and Info Stealer Malware



Another common way credentials are compromised is via various forms of malware or spyware, particularly keystroke loggers. As the name suggests, this type of malware records and sends to the fraudster a data log of all characters typed as or after the user has used their computer. The idea is that the key-stroke logger will capture and relay the usernames, email addresses and pass-words the user presents to a multitude of sites at login events. This information is then used by the fraudster to access the malware victim's accounts.

Like phishing and data breaches, keystroke loggers provide the credentials for a bad actor to use directly or sell to others on the dark web. The organization allowing the real user to sign will have no idea that user has this malware active on their device but could very likely see those stolen credentials used in stuffing attack later.

Other types of malware beyond keystroke loggers have also been used successfully to bypass or beat 2FA. Info stealer malware is a problem in particular, as it can be used to execute web session hijacking or cookie hijacking attacks. In these attacks, the malware is able to obtain session cookies and possibly assume a users' web session. This may be used to bypass login entirely, or may make the attacker appear to be coming from a trusted device that is able to avoid being prompted for 2FA.

Advanced Phishing

High-value accounts, such as investment or brokerage accounts, online banking and workplace logins, are very often targeted with sophisticated adversary-in-the-middle (AiTM) attacks.

With advanced phishing, attackers are targeting users who they already know are customers of a particular website and may have already obtained valid credentials for specific victims (perhaps having purchased them, or using precursor credential stuffing attacks as discussed earlier). Users are fooled into visiting fake versions of targeted websites that contain sophisticated phishing kits that launch what are known as adversary-in-the-middle (AiTM) attacks.

With AiTM attacks, the phishing kit isn't just collecting credentials and 2FA codes from the victim, it's actively proxying them to the legitimate site and leveraging them in real-time to achieve a fully authenticated session with the legitimate website and obtaining the session cookie that is associated with the authenticated session. Even a relatively novice fraudster is able to pull off AiTM attacks by purchasing malware kits, while these attacks frequently target high-value accounts.

Obtaining a working session cookie is particularly problematic, as that cookie can be used (often for an extended period of time) by anyone to obtain access to the compromised account without having to re-authenticate and without any need to complete 2FA processes that are enabled on the account.

Challenges for Consumer eCommerce: 2FA Exhaustion and Operational Costs

When given the choice to opt-in, most consumers will NOT activate 2FA for their accounts with eCommerce merchants.

When discussing credential stuffing attacks above, this was grounded in the best-case scenario: that 2FA was presented and it stopped the unauthorized account access from occurring. However, that assumption is not a luxury most eCommerce merchants can afford because they are typically not going to force 2FA on all users or on all login attempts.

Typically in the B2C eCommerce space, 2FA is an opt-in choice for users, if offered at all. Some organizations may selectively use 2FA such as after multiple failed login attempts or turn it on only once bot activity has been identified. The reality for eCommerce merchants is that 2FA needs to be used selectively, if not sparingly, for two primary reasons:

It doesn't make sense in terms of operational costs to require 2FA on every log-in event when many to most don't end in a revenue-generating event, and this extra friction would likely cause churn.

1. **To reduce the operational cost of 2FA, only presenting it when there is a valid case to do so**
2. **To protect UX amidst 2FA exhaustion**

Simply put, not all log-ins at a merchant website result in a transaction or event that drives revenue, therefore operational risk management costs around non-revenue generating events need to be minimized. It doesn't make financial sense to always require 2FA unless you are a financial institution or other organization that is protecting sensitive information or access to spendable funds. Most merchants, on the other hand, are going to delay more risk screening until an event with the potential for financial gain or loss transpires, because in many cases it will not.

Passive solutions used to dynamically determine when to present 2FA save most users from the 20 to 25 seconds it takes them to complete this process.

More important of a factor, however, is that most consumers simply won't tolerate 2FA ubiquitously. They are suffering from 2FA exhaustion and may decide to simply not continue with the login process rather than take that extra step if 2FA is required too often. Consumers are often annoyed when 2FA is prompted, and understandably become frustrated when it does not go smoothly, such as an SMS-based passcode arriving late or not at all. According to a research paper titled "A Usability Study of Five Two-Factor Authentication Methods" published by USENIX[3], the average time to complete 2FA is 18.5 seconds for SMS authentication and 23.9 seconds for time-based one-time password (TOTP) services like Google Authenticator. That is not acceptable to the average consumer, which is why they typically won't opt-in, or won't log-in, if it is forced upon them.

More passive solutions are better, both in terms of UX and operational expense. Forcing 2FA for all is costly and will cause churn. Offering 2FA as an option will only get a small subset to opt-in. A better option is to utilize services that look for the use of compromised credentials and detect credential stuffing attacks. This provides the insights that drive more strategic actions in terms of when to throttle activity, or when to force a password reset because there is meaningful risk that it is not the authorized user presenting the correct credentials.

"Consumers, when faced with better security options at the cost of higher friction, will choose lower friction options. This is why on sites with opt-in 2FA some of the most at risk accounts will never opt in for this level of security. Surveys indicate that more than 70 percent[4] of consumers choose NOT to enable two or multi-factor authentication for their social media accounts or cryptocurrency accounts, with opt-in rates even lower in other industries."

David Montague

CEO, myNetWatchman

Sources:

3 - https://www.usenix.org/system/files/soups2019-reese.pdf

4 - https://www.prove.com/blog/prove-identity-2023-state-of-mfa-report-consumer-attitudes-multi-factor-authentication

Recognizing ATO Attacks

The ATO that most organizations are aware of is just the tip of the iceberg.

Cases of account takeovers that cause a direct financial loss are more likely to be caught, but this isn't a guarantee. Successful ATOs that result in scraping PII or accessing services are much less likely to be seen. It's likely that the vast majority of failed ATO attempts are just seen as failed logins, not necessarily ATO. Many users who realize they fall victim to ATO never report it to the organization, they just stop using the site or service. The extent of ATO activity is not fully seen, but that doesn't make it any less damaging.

There are several signs organizations can look for to detect that ATO activity is occurring and to identify spikes in ATO attempts during attacks. If using 2FA, even just for users who opt-in or when it is used selectively, look for spikes in login attempts that provide a successful password but do not pass the step-up to two factor authentication. This should not only look at 2FA failures (when the wrong OTP is provided), but also sessions that do not attempt to pass the 2FA. The latter could be indicative of credential stuffing attackers who are just looking to validate that the credential is active on your site, or it could be a fraudster who doesn't bother trying to pass the 2FA check because they haven't compromised the second factor.

While firewalls might be effective against high-volume brute force attacks, they are less effective at stopping credential stuffing attacks, which cycle through IPs or proxies and space out the login attempts to better evade detection.

To help detect ATO attempts when 2FA is not presented, look for constant flows of failed login attempts as well as spikes in login attempt and failed login activity. Credential stuffing tends to be systematic where you may see login attempts occur at a consistent interval while each username and password is only attempted once. Credential stuffing attacks can also use bots designed to tumble passwords that adhere to various password policies, such as adding the number 1 or a different special character to the end of the root password that was compromised.

The last way an organization wants to find out about an attack is from their customers, but take reports of targeted phishing campaigns and social engineering seriously. If a specific user is targeted by a phishing campaign mimicking an organization's logos and email format, it is highly likely that the targeted users are known to hold accounts with that organization. Also keep in mind that most consumers will not report this activity to the organization being mimicked in the phishing attack, so for every event report count on there being dozens more that weren't. Spikes in these kinds of reports from users are meaningful as they show a systematic and large-scale attack is underway.

Organizations stand to benefit from services that look for the use of compromised credentials and detect stuffing attacks. These insights provide protection against ATO while improving the user experience through reduced use of step-up authentication, which injects more friction in the login process each time it's presented.

Conclusion

Online and multi-channel merchants are often well-versed in risk management at the transaction event and understand that effective risk management requires striking a balance. They must balance the cost of fraud prevention services and how stringent their fraud prevention policies are, such that it does not adversely impact legitimate customers and sales conversion.

myNetWatchman customers benefit from a repository of over 30 billion exposed user credentials and ten years of live data surveillance. Clients leverage these insights to passively make dynamic, risk -based decisions across each login attempt.

A similar approach and focus on balancing risk management with the user experience is required when it comes to the login event as well. This starts with protecting the first factor of authentication: the password. While 2FA may be effective in preventing unauthorized account access, it doesn't fully protect the user base from bad actors confirming the compromised credentials they possess are valid. Further, 2FA is disruptive to the user experience and most consumers will not choose to use it unless they are forced to, while requiring 2FA is not the standard in eCommerce retail.

Multi-channel and eCommerce merchants therefore need more passive solutions to understand log-in risk and protect users from their own reuse of compromised credentials. myNetWatchman's data repository of over 30 billion exposed credentials and live data surveillance protecting over 600 million users provides unique and powerful insights that organizations leverage to make dynamic, risk-based decisions on a per user and per log-in basis.

Are you looking for answers or solutions, for eCommerce payments and fraud management? Give us a call for a free introductory consultation to see if we can help you. Even if we can't meet your needs we most likely know someone who can, and we are happy to provide you with contacts of reputable firms and individuals servicing the space.

About the Fraud Practice

The Fraud Practice is a privately held company based in Palm Harbor, Florida. The Fraud Practice provides training, research, and consulting services on eCommerce payments, fraud prevention, and credit granting. Businesses throughout the world rely on The Fraud Practice to help them build and manage their fraud and risk prevention strategies.

For more information about The Fraud Practice's consulting services, please visit www.fraudpractice.com. For additional information about The Fraud Practice's online training programs, please visit www.OnlineFraudTraining.com.

The Fraud Practice
www.fraudpractice.com
www.OnlineFraudTraining.com
Telephone: 1.941.244.5361
Email: Questions@fraudpractice.com

About myNetWatchman

Georgia based myNetWatchman has been providing cyber fraud intelligence data for more than 20 years to retailers, financial services, insurance, and other industries. With over 10 years of live data surveillance, the company manages a continuously growing data repository containing over 30 billion exposed credential pairs and protects over 550 million users for their clients.

myNetWatchman
https://www.mynetwatchman.tech/
Telephone: 678-624-0924
Email: contactus@mynetwatchman.com

THERE IS NO SILVER BULLET: USER CREDENTIALS ARE NOT SECURED WITH 2FA ALONE

White paper by The Fraud Practice and myNetWatchman
Sponsored by myNetWatchman