www.pipelinepub.com
Volume 20, Issue 1

Hackers Unmasked: How they Use your Identity Against you

By: Xavier Salinas

In my 15-year career in the world of IT and cybersecurity, the attack surface used by hackers has continually grown while we have more and more to protect. Simply put, the more we innovate and advance, the more ways "in" hackers have. While the cloud remains a prime target for hackers today, earlier in my career the focus was on targeting network perimeters, critical internet-facing vulnerabilities, and endpoint devices. Now, the emerging attack surface is single sign-on (SSO). While SSO eases friction for its users, it also makes hackers' lives easier. Because it is mainly stored in third- party cloud environments, it is also difficult to audit. Altogether, the inherent risk of SSO can have terrifying ramifications!

Single sign-on is like having a master key that unlocks your house, car, and office. It simplifies your online experience by allowing you to access multiple applications and services with just one set of credentials, sparing you the hassle of remembering multiple usernames and passwords. It is used by Microsoft, Google, Apple, Amazon, Facebook, Okta, Duo, and more. That's right—it has become part of our personal and professional lives. For instance, when you log into your email, SSO seamlessly grants you access to your cloud storage, project management tools, and collaboration platforms without the need for repetitive logins. It is the magic wand that streamlines your digital journey. However, while this convenience is undoubtedly appealing, it comes with its own set of challenges and security threats. In this article, we examine five identity-based threats—Artificial Intelligence (AI), the inherent risk, vendors' security, multifactor authentication bypass, and human error—to help you approach SSO with appropriate caution.

The Utilization of AI Within Cyberattacks

Picture this: you receive an email that seems to be from your bank, asking you to confirm or provide information. It looks convincing, just like a real email from your bank. But guess what? It's not from your bank; it's from a hacker who is using AI to make their phishing emails look legitimate. They have

fixed all the grammatical errors and spelling mistakes, making it nearly impossible to tell them apart from genuine messages. With generative AI, hackers of all experience levels can carry out such attacks.

And that's not all. Hackers also use AI to manipulate their voices, making them sound like someone you trust. Essentially, they back up their emails and phishing schemes with a call or voicemail. Whether it's the reassuring tone of your bank's representative, the authority of your boss, or the familiarity of a family member, these voices coax you into gaining a false sense of security. Therefore, you are more likely to provide sensitive information or money—just what the hackers want.

These phony emails and phone calls are not just standalone attacks; they serve as the first step to hacker cyberattacks. Once they gain your trust and manipulate you into taking a seemingly harmless action, they're in. With that initial breach, they can potentially gain access to your SSO credentials, then access your entire personal or professional online presence, or worse, both.

Inherent Risk

While single sign-on as your digital master key is convenient, that convenience comes at an inherent cost. Like you, hackers only need that one key to get in. They can then use SSO as a launch point to get into connected online services. To illustrate the real-world impact of this, consider the reported case of MGM Resorts. Here, the ALPHV group used a simple yet ingenious tactic. Posing as an employee, they placed a phone call to MGM Resorts' Help Desk and tricked their way into gaining access. Once inside, they targeted the SSO system, used it as a launch point, and gained access to servers, machines, and more. What began with a 10-minute phone call led to an estimated loss of $100M for MGM. While SSO is convenient, it can thus also be a high-value target for cybercriminals, providing them with a shortcut to a vast array of sensitive data. Most of us have been targeted by these simple tactics and a lot of us know someone who has fallen victim to similar phishing and social engineering scams. They are all too common, and, frankly, all too simple.

Dependence on SSO Vendors' Security

Using SSO requires working with a third-party vendor—and relying on the degree of security the vendor offers. Relying on vendors' security, however, poses risk for a couple of reasons.

First, if a vendor's product has a security weakness or gets hacked, it could lead to a supply chain attack. This is when a hacker strategically targets a vendor intending to gain unauthorized access to the vendor's systems, as well as their clients' accounts and data. It is like a hacker getting a hold of one master key for the vendor and for all of its clients. The consequences can be dire, especially when sensitive information or valuable assets are at stake.

Second, dependence on SSO vendors can lead to distributed denial of service (DDoS) attacks. In such an event, an overwhelming amount of traffic floods the victim's environment, making it incapable of functioning properly, and thereby preventing both vendor and clients from accessing the services and data they rely on for daily operations.

If an SSO vendor's security infrastructure is compromised or experiences downtime due to a cyberattack, the repercussions can be far-reaching. It not only jeopardizes online safety but also has the potential to disrupt productivity.

Multifactor Authentication Bypass

A part of the login process that often follows a single sign-on prompt is multifactor authentication (MFA). It is like having a deadbolt lock in addition to the master key. That way, if hackers successfully acquire your SSO credentials, they may still be thwarted at the MFA prompt. But here's the catch—they've figured out how to bypass that deadbolt. They may do so by:

- Stealing browser tokens
- Intercepting your MFA prompts or codes
- Sending you repeated MFA notifications till you accept out of annoyance
- Pretending to be you in order to reset, and therefore access, your MFA.

Although MFA bypass is an unfortunate reality, it is still better to have MFA than not. Without MFA as your deadbolt, hackers truly only need that one set of credentials to gain access to everything. When using MFA, I recommend biometric authentication, hardware keys, app-based solutions, or push notifications with number matching over SMS-based MFA.

Human Error

Let's face it—we're all human, and humans make mistakes. Single sign-on setup and maintenance can be complex, and it is easy to make mistakes. If you make a wrong move, you may accidentally hand the master key directly to a hacker.

In fact, one of the biggest threats to identity-based attacks is the human element. Over-privileging accounts, accidental deletion, misconfiguration, data corruption, and unintentional data exposure happen more often than you may think. More often, in fact, than ransomware attacks.

Securing data, including your SSO, in the cloud is a shared responsibility. Businesses and their cloud service providers both have roles to play. While service providers are responsible for securing the actual cloud, businesses are responsible for securing what they place in the cloud. For instance, it's the job of businesses to configure platforms and resources and manage access. Teamwork is required for success, and we all play a part in using tools such as SSO wisely.

Conclusion

Single sign-on offers a convenient, one-key-fits-all digital-age security solution. This convenience, however, comes with its own set of challenges. These five identity-based threats warrant consideration when embracing the benefits of SSO:

1. Utilization of AI in cyberattacks
2. Inherent risk
3. Dependence on SSO vendors' security
4. Multifactor authentication bypass
5. Human error

While having a master key can be convenient, it is essential to be aware of the risks and ensure that our digital lives remain secure. Acknowledging these five identity-based threats and taking proactive security precautions accordingly can enable us to strike a balance between convenience and safety in our digital world. In doing so, we can continue to enjoy the benefits of SSO while safeguarding our digital lives from harm.