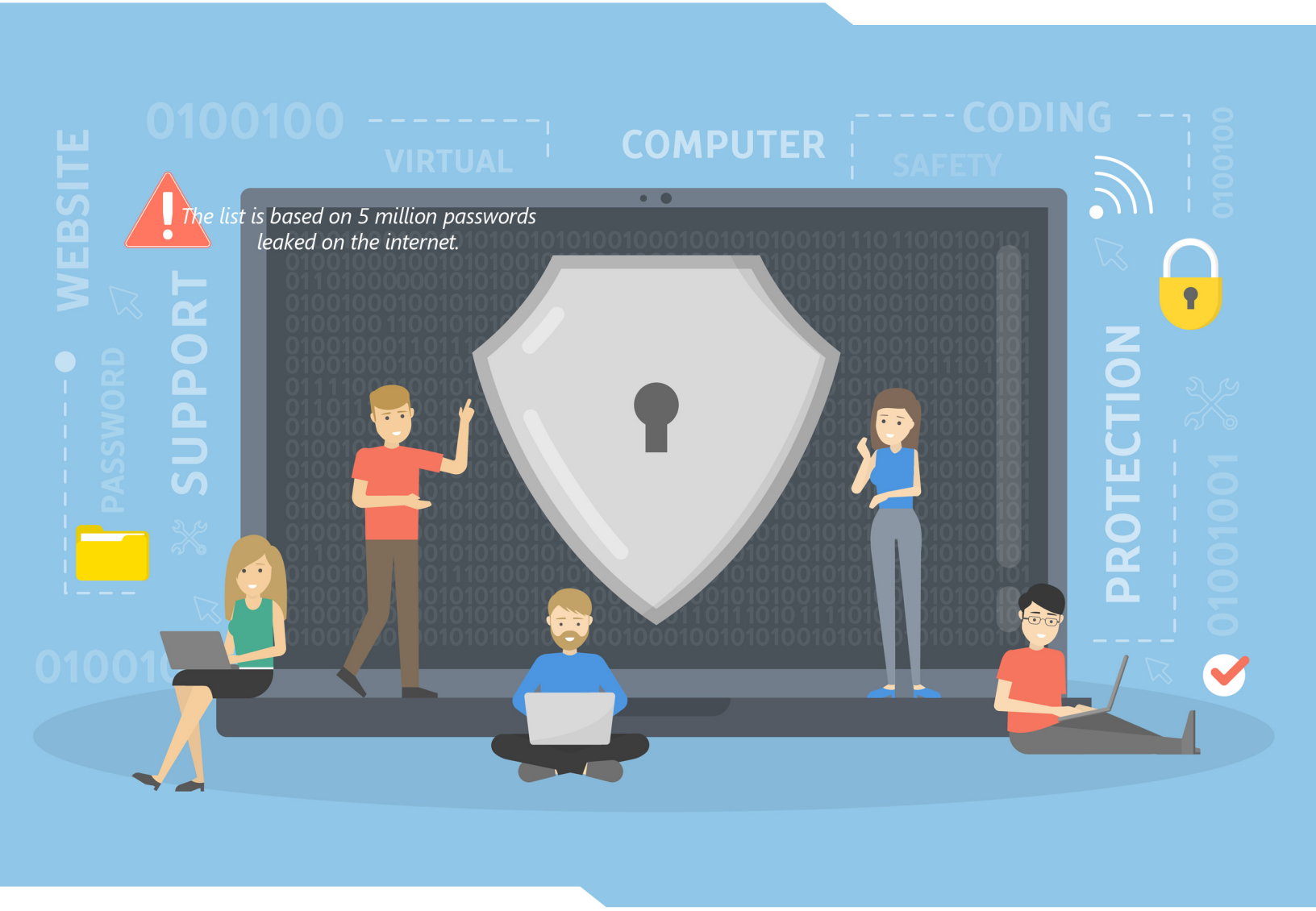
Discovery
INFORMATION TECHNOLOGIES
We Make I.T. Happen!



How Do We Keep Our Information Private?

There Are 12+ Ways To Hack Two-Factor & Multi-Factor Authentication

All forms of multi-factor and two-factor authentication can be hacked. This can even be done by a hacker simply sending you a phishing email. How can you defend your business from these attacks? How can you keep your information private? Multi-Factor Authentication (MFA) at one time was only used for the highest security needs. Today, with the increasing prevalence of cyber threats and sophisticated hacking, it's being used by everyday organizations and businesses.

(409) 727-7080 • Info@discoveryit.com
discoveryit.com • 904 Hwy 69 N • Nederland, TX 77627

Discovery
INFORMATION TECHNOLOGIES
We Make I.T. Happen!

We've been told that we can trust the security of MFA, and for the most part we can. It's been effective for computer defenses and can defeat many of the threats that would have been successful against single-factor authentication solutions. All businesses should use MFA solutions instead of single-factor authentication solutions to protect sensitive data.

However, the ability of MFA to eliminate all security risks has been overstated to some degree resulting in some users believing that email phishing isn't a threat when it comes to MFA. They think that they can't be phished out of their login credentials. This isn't true.

While MFA does reduce the risk, many attacks that are successful against single-factor authentication can also be used successfully against multi-factor and two-factor authentication. We'll explain 12 ways that MFA and 2FA can be hacked. And we'll also explain how you can defend against these attacks.

What Are The 12 Ways To Hack MFA & 2FA?

A primary way is to find weaknesses in the entire authentication process, including identity registering, authentication secret storage, authentication, and authorization. But, before we get into this, let's go over what authentication involves.

What Is Involved In Multi-Factor Authentication?

This the process of proving ownership of a particular identity. Authentication is the process of a person proving ownership of an authentication identity. This identity is usually something like a login name, email address, or a series of characters. Namespaces are used to collect information to authenticate a user's identity.

The identity should be different than what is being provided to prove ownership of the identity. For example, in Microsoft Windows, although you might use a fingerprint to authenticate, the label attached to an authentication attempt will probably be your login name or email address.

There Could Be Issues With The Storage of Authentication Proof

The problem can be in the way the authentication proof is stored. The authentication proof is often not stored on the server/service/site directly involved in the authentication. Instead, it's stored on a third-party server/service/sites involved in the authentication.

Unfortunately, each storage location is a potential attack vector for compromising authentication. It's important that you think about where your authentication proofs are stored, who has access to them, and how trustworthy the storage is. Plus, storage of authentication secrets should be restricted to the minimum number of administrators required. It should also be aggressively monitored and audited. If the authentication secrets are compromised, the authentication process can't be trusted.

After successful authentication, in many instances, an access control object like a token or code is provided. This could be a series of numbers or characters. And after the successful authentication, the person can often use the token for the rest of the authentication cycle.

The token may or may not have a pre-determined maximum lifetime. If it expires, the person has to re-authenticate to stay in a session. However, in some cases, once an access control token has been issued, authentication isn't tested for each and every authorization access attempt. This is because possession of the access control token is considered the proof for successful authentication. And if an attacker can access the control token, the site doesn't care how you authenticated.

Possession of the token, whether it's legitimate or not is usually treated by authorization processes the same way. This means the hacker holding the token can successfully authenticate. The authorization process doesn't know that a hacker is using the token, and hackers know this.

What Do Hackers Look For?

This same concept applies to the entire authentication process. Hackers look for weaknesses in the authentication process as a whole. They will search for security gaps between identity, authentication, and authorization.
This is why most companies that use MFA and 2FA can still be successfully hacked.

What Are The 12+ Ways Hackers Hack MFAs & 2FAs?

In general through:

- Social Engineering (the human element)
- Technical (manipulation that doesn't require a human mistake)
- Mixed (a mixture of both)

1. Session Hijacking

This is where after a successful and legitimate authentication your session is hijacked by a hacker. This usually happens when a token is stolen. You might not know that this has occurred. You may have accidentally responded to a phishing email. Regardless of how the hacker hijacked your token, now they can take the session away from you to steal your confidential information. This is one of the most common forms of MFA hacking.

2. Session Unique Identifier Prediction

Every time you authenticate using MFA you get sent back a session token to use as your unique identifier. But it's important that this identifier isn't predictable enough for a hacker to guess what it is.

Session hackers look for websites that use predictable identifiers. They join the websites they are targeting and look for similarities between the unique identifiers. Sometimes they aren't random enough and are sequential in order. The hacker recognizes the pattern and tries using different numbers to see which one will work.

With or without the MFA being used, if the hacker can predict the unique identifying information they can become the "user." Unfortunately, not all website coders are aware of this problem.

3. Session Hijacking Proxy Attack

Here the hacker must first successfully establish themselves in between the client and server like in a man-in-the-middle attack (MitM)). This isn't as difficult as you might think and can be done locally in any shared wireless network (like when you use public WiFi).

Or the hacker can do this across the Internet by sending the victim a phishing email to entice them to visit a fake "look-alike" or "sound-alike" website. Once you've been a victim of this kind of attack, everything you send can be intercepted by the hacker.

Note: Your session identifiers must be unique and randomly generated.

4. Phish Around

The hacker can phish around a victim's MFA solution:

1. They set up a fake look-alike/sound-alike website that was really an evil proxy site.
2. They trick the user into visiting the evil proxy website.
3. The user types in their credentials and the hacker can now pretend to be the legitimate customer.
4. The legitimate website sends back a session token that the hacker steals to take over the user's session.

Be sure to use mutual, 2-way authentication and educate your staff on how to avoid social engineering attacks.

5. Fake the Authentication

One of the easiest ways to hack MFA is when the entire authentication experience is fake. You're tricked into visiting a site that you have an MFA token for. The fake site looks like the legitimate one. You put in your login name and password.

The fake website can also ask for additional security information to "qualify" you, such as social security information, credit card information, etc. After capturing your confidential information, the hacker then makes it look like the website experienced an error and sends you off to the real website, so you never know what happened. This hack can even be used to then log into another legitimate website that you use. This type of MFA attack is very difficult to avoid because the MFA solution isn't really being hacked.

6. Man-in-the-Endpoint Attacks

If the attacker gets admin access on a device, nothing you do on the device can be trusted. The hacker can do anything that you can do. They have essentially piggybacked onto your authentication. A “local” hacking can even steal your session tokens and mimic the attacks described above without having to do a Man-in-the-Middle attack first.

7. Banco Trojans

A Man-in-the-Endpoint attacker can also open another hidden browser session while you are in the first session. They use banking trojans (bancos trojans) which are commonly used in South America. The bancos trojan can exploit a local computer using any method that traditional malware uses (such as phishing). Then the trojan monitors your browsing looking for keywords, such as "bank," "Bank of America," etc.

When the bancos detects that you are is logging into the financial institution site, it starts a second, hidden, browser session. And all the while the bancos trojan is changing your contact information and initiating a large wire transfer of funds to a rogue bank account. If the bank calls or emails to confirm, they use the new fraudulent contact information. MFA approval messages should always be sent from the bank with details about the transaction so you can see them before approving it.

8. Malicious MFA Software Modification

If a hacker has admin access to your device or operating system, they can do anything on your hardware or software. All MFA solutions use software. Even if you don't install and "initialize" your MFA option in the software, it was already enabled by default.

Hackers will try to modify the MFA software program to weak or disable it. Or they compromise your network node and steal keys you used to encrypt communications. Now they can read all of your encrypted content. Make sure your software is fully patched. It’s essential to ensure your employees don’t get tricked into installing malware on devices.

9. Malicious MFA Hardware Modifications

Sometimes MFA hardware solutions have been physically modified to not provide typical protection. And sometimes, predefined encryption keys were directed toward the intended targets. The targets use the MFA solutions thinking they are completely secure. But they aren’t.

10. SIM Swaps Attacks

Most cell phones use small memory cards known as Subscriber Identity Modules (SIMs). It also holds data in your phone including application data. Hackers have been stealing subscriber's SIM information and transferring it their own phones.

This has been done in-person when the hacker goes to the cellphone store and pretends to be the subscriber wanting to upgrade or replace his cell phone. They can also do this remotely via the cellular network provider’s tech support. In other cases, employees at cell phone stores have even been bribed to participate in the SIM swaps. When the SIM swap happens your phone will stop working, and the hacker has every text message sent to your phone.

11. SMS Rogue Recovery

SMS message origination legitimacy can't be authenticated. So anyone can claim to be a legitimate sender. (Much like in a phishing email.) Hackers can send rogue instructions to unknowing victims. They only need to know your email address and phone number. They can send you a fake SMS recovery message claiming to be your email provider. The message says they require that you send an authorization code to access your email account.

Next, the hacker sends your email account into SMS recovery mode by pretending to be you. They take the legitimate recovery SMS verification code and type it into the email provider's web form, and take over your email account.

12. Duplicate Code Generators

Many MFA solutions use code generators where you're presented with a time-sensitive code to validate your identity. They often appear as random digits or characters, and you must enter them within 30 to 600 seconds. When you do this, your device is uniquely identified (ex., Serial number, etc.) with a "seed value." It's then stored in one or more controlling authentication databases. If an attacker accesses the seed value database, he takes the seed value and uses it to create valid time-sensitive codes to get into your accounts.

These are only 12 ways that hackers can hack into your two-factor or multi-factor authentications. There are others, and we'll be happy to discuss them with you. In the meantime here's a summary that you should keep in mind.

- **MFA isn't unhackable.**
- **MFA doesn't prevent phishing or social engineering from being successful.**
- **MFA is good. Everyone should use it when they can, but it isn't 100% unbreakable.**
- **If you use or consider using MFA, security awareness training has still got to be a big part of your business' overall security defense.**