BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle
November 2019

Two-Factor Authentication

Two-factor authentication (2FA), also referred to as Multi Factor Authentication (MFA), is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor authentication, such as just providing a password or passcode to authenticate your email or user ID. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan.

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's email, devices, or online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online service providers are increasingly using 2FA to protect their users' credentials from being used by hackers who have stolen a password database or used phishing campaigns to obtain user passwords.

What are authentication factors?

There are several different ways in which someone can be authenticated using more than one authentication method. Currently, most authentication methods rely on knowledge factors like a traditional password, while two-factor authentication methods add either a possession factor or an inherence factor.

- A **knowledge factor** is something the user knows, such as a password, a PIN or some other type of shared secret. Your Mother's Maiden Name, your first pet, and so on are examples of these. But a lot of this information is now available online with the prevalence of social media and on the dark web.

- An **inherence factor**, more commonly called a biometric factor, is something inherent in the user's physical self. These may be personal attributes mapped from physical characteristics, such as fingerprints authenticated through a fingerprint reader; other commonly-used inherence factors include facial and voice recognition. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns.

- A **possession factor** is

(Continued on next page)

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

2FA (Cont.)

- something the user has, such as an ID card, a security token, a smartphone or other mobile device. This has become the most popular method such as a random set of numbers you need to enter, that change every 30 seconds, and are displayed and tied to only your cell phone.

Other authentication and security methods used in some applications like Office 365 include:

- A **location factor**, usually denoted by the location from which an authentication attempt is being made, can be enforced by limiting authentication attempts to specific devices in a particular location, or more commonly by tracking the geographic source of an authentication attempt based on the source IP address or some other geolocation information derived from the user's mobile phone or other device such as GPS data. Such as only allowing login to your email from the United States.

- A **time factor** restricts user authentication to a specific time window in which logging on is permitted, and restricting access to the system outside of that window. Certainly hackers may spend more time trying to get in during off hours like night and weekends.

It should be noted that the vast majority of two-factor authentication methods rely on the first three authentication factors though systems requiring greater security may use them to implement multifactor authentication, which can rely on two or more independent credentials for more secure authentication.

What is two-factor authentication?

Two-factor authentication is a form of multifactor authentication. Technically, it is in use any time two authentication factors are required to gain access to a system or service. However, using two factors from the same category doesn't constitute 2FA; for example, requiring a password and a shared secret is still considered single-factor authentication, as they both belong to the same authentication factor -- knowledge.

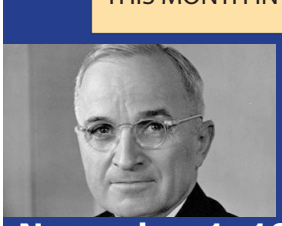
As far as single factor authentication services go, user ID and password are not the most secure. One problem with password-based authentication is it requires knowledge and diligence to create and remember strong passwords. Passwords require protection from many inside threats, like carelessly stored sticky notes with login credentials, old hard drives and social-engineering exploits. Passwords are also prey to external threats, such as hackers using brute-force, dictionary or rainbow table attacks.

Given enough time and resources, an attacker can usually breach password-based security systems. Passwords have remained the most common form of single factor authentication because of their low cost, ease of implementation and familiarity. The addition of Possession factor authentication can provide more security using an Authentication app on your individual cell phone, can provide a more secure method of keep your login accounts and email safe.

FACT FILE

DID YOU KNOW?

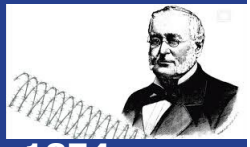
THIS MONTH IN HISTORY



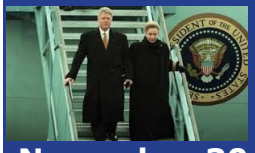
November 1, 1950 - President Harry S. Truman was the target of an unsuccessful assassination attempt by two members of a Puerto Rican nationalist movement.

November 11, 1938 - Irving Berlin's God Bless America was first performed. He had written the song especially for radio entertainer Kate Smith who sang it during her regular radio broadcast. It soon became a patriotic favorite of Americans and was one of Smith's most requested songs.

November 20, 1789 - New Jersey became the first state to ratify the Bill of Rights.



November 24, 1874 - Joseph Glidden patented his invention of barbed wire.



November 30, 1995 - Bill Clinton became the first American president to visit Northern Ireland.

Watch Out For Old Hacking Technique Offering Free Downloads

An old hacking technique is getting new attention from hackers around the world, and it underscores the fact that people must exercise extreme caution when it comes to deciding who to trust and where to download files from.

Hackers have long been in the business of spoofing legitimate sites; making exact replicas of popular websites offering a variety of free downloads.

Of course, instead of getting genuinely useful code, you find yourself on the poisoned domain. Rather than the legitimate site, what you download will be malware of one type or another.

The most recently discovered instance of this involves the Smart Game Booster site. It's a legitimate piece of code that helps to improve the performance of the games you play, and it has become popular enough that it's caught the attention of at least one hacking group. That group cloned the site and pretends to offer the same product.

In this case though, the malware the hackers deploy is one of the more insidious we've seen. Unlike many malware attacks which latch onto a system with a persistent presence, this one runs only once and then deletes itself. Even more alarming is that it leaves no trace that it was ever there.

When it runs, it scans the infected device for passwords, your browser history, any cryptocurrency wallets you may have, and a wide range of other critical files. It collects these and sends all the data to its command and control server, and then self-destructs.

With no outward sign, many users will be completely unaware that there's a problem until they start seeing suspicious charges on credit cards, noticing funds being removed from bank accounts and the like. By then of course, it's far too late.

The bottom line here is simple: Be mindful about where you download files from. Check your URLs, and unless you can avoid it, never stray far from the big, well-respected sites like the Apple Store, Microsoft Store, or Google Play Store. It's just not worth the risk.

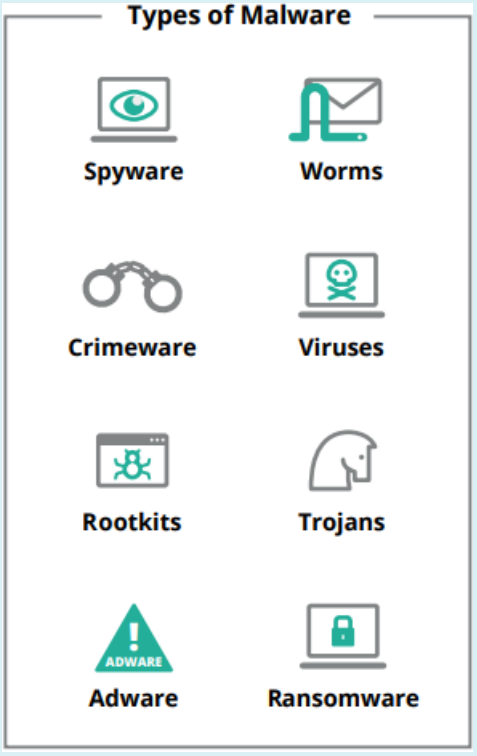
There are plenty of things that can go wrong if you click on a bad link or download an infected file, and Malware is another one of those things. Malware or malicious software comes in many forms and is harmful to the system it infects.

Malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Malware likes to make money off of you and will often hold your device, or files at ransom.

How to prevent your devices from being infected with malware:

- Beware of suspicious looking domain names
- Avoid interacting with pop up ads
- Keep your operating system and antivirus up to date
- Only download apps from the app stores
- Do not click on strange links

Stay vigilant, and always think before you click.



RANSOMWARE ROUNDUP

Alive and well, ransomware continues to terrorize organizations and entities all over the world. Attackers have spread their campaigns from large corporations to schools, city governments, small businesses, and even individuals.

What is ransomware?

As the name suggests, ransomware is a form of malware that encrypts files or locks computers until a specified ransom is paid in full. Cybercriminals threaten to destroy the encrypted data if the ransom isn't met by a predetermined date.

How do ransomware infections happen?

Someone clicked on something! In almost every case, ransomware was made possible by malicious links or attachments sent via email. In a small percentage of attacks, cybercriminals successfully manipulated security holes to inject the malware into a network without human interaction, but that is rare.

Why is ransomware so popular?

Unlike traditional data breaches, which result in stolen information, attackers use ransomware to lock up crucial systems. They know that most entities will pay to have those systems restored. For example, a city in Florida paid a steep price to regain control of their systems, which included emergency dispatch services. Ransomware provides a quick and healthy payday in a way that even the largest data breaches can't.

Preventing Ransomware in 3 Easy Steps

First things first–preventing ransomware and other cyber-attacks begins and ends with following our organization's policies. They are designed to protect all of us, and circumventing policies, for any reason, puts us at risk. With that in mind, follow these three steps to prevent ransomware in your personal life, and if you have any questions about our policies here at work, please ask!

1. **Stay alert for phishing attacks.** Some are easy to spot thanks to obvious indicators like poor grammar, bad spelling, and threatening language (like claiming your account has been suspended or that you owe a delinquent tax payment). Other attacks use more sophisticated techniques, such as sending an unpaid invoice to someone. No matter what, think before you click, and stay alert!
2. **Keep systems up to date.** Even if ransomware rarely spreads via security vulnerabilities, outdated systems are begging to get hacked. Enable auto-update on all of your devices and apps so you never miss an important security patch.
3. **Back up your data.** Security researchers recommend that you keep at least two redundant copies of your data and store one of those copies at a second location (such as the Cloud). There are plenty of free programs that will manage your backups and run automatically. But to fully shield yourself from ransomware, consider storing a backup offline so it doesn't get impacted should you run into ransomware.