CONCENSUS
TECHNOLOGIES

STAYING SAFE WITH MULTI-FACTOR AUTHENTICATION

DON'T BE AN EASY TARGET

Previously, we had the luxury of passwords being sufficient most of the time. Unfortunately, this is no longer the case.

The way and means to steal a password has become technologically advanced. Individuals and small to medium-sized businesses are being specifically targeted. Passwords can now fall into the hands of anyone on the net. So, we all, individuals and businesses alike, need an additional means of protection.

This is where Multi-Factor Authentication comes in.

"ADDING THAT SECOND LAYER OF AUTHENTICATION IS A LOW-COST, PROVEN SECURITY SOLUTION YOUR BUSINESS CAN EMPLOY TO PREVENT 99.9% OF ACCOUNT COMPROMISE ATTACKS AND AVOID A DATA BREACH." (Systems Engineering)

What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is an extra means of security to verify a user's identity.

Specifically, in addition to a username and password, MFA requires at least one other credential before granting a user access to a system.

By requiring multiple credentials, any system or application knows that you are, indeed, who you say you are. Credentials can vary, depending on security issues, clearances, or other concerns.

Types of credentials come from:

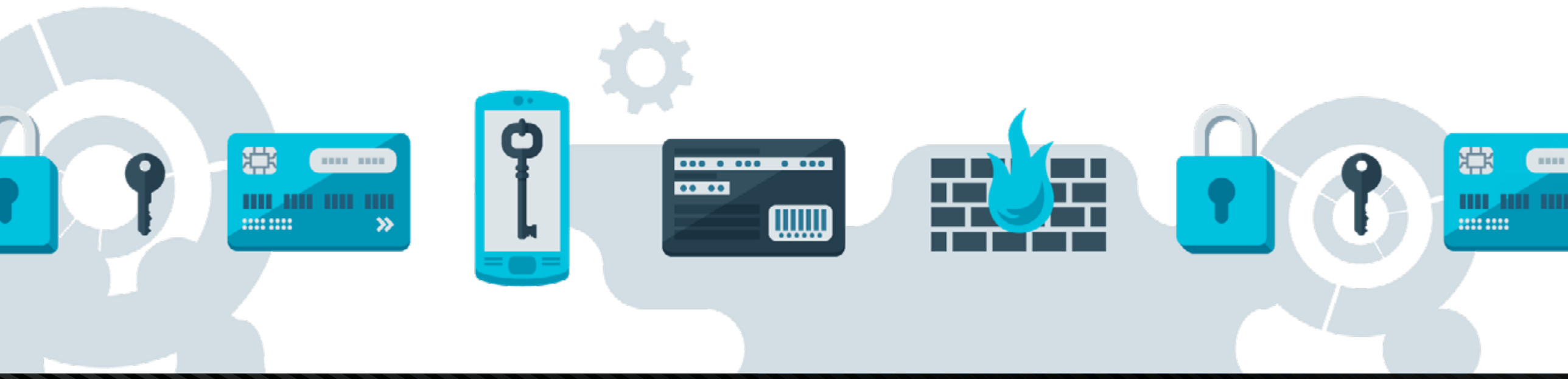
- **something you know (PINs, Security Questions),**
- **something you have (fob, card, or smartphone),**
- **something you are (thumbprint, voice or facial recognition)**

For instance, MFA may use a verification code sent to the user's smart-phone, require answers to a set of security questions, or may be a series of more intricate security measures depending on the level of access required. With MFA, it is exceptionally unlikely, that a malicious person, will know or have access to, the second set of credentials.

You may already use MFA quite frequently, for example:

- **ATM's – When using an ATM, you need your PIN and your card. It is only under duress that someone can steal and use both.**
- **Passports – Typically, these need various forms of ID such as a birth certificate, a driver's license and even a photo for facial identification.**
- **Changing Passwords – Depending on the app, when you change or alter your account, a verification code is sent to your email, smartphone or via a phone call.**
- **Office Access – Many offices grant access only if you have a fob or access code to enter the building and then another PIN or key to enter the actual office.**

**It is important to note that since passwords are compromised, having two passwords is not sufficient and not part of MFA.



Why Do I Need MFA?

MFA is the most effective way to prevent credential theft

"CREDENTIAL THEFT AND SOCIAL ATTACKS SUCH AS PHISHING AND BUSINESS EMAIL COMPROMISES CAUSE THE MAJORITY OF BREACHES (OVER 67 PERCENT), AND SPECIFICALLY:

- **37 percent of credential theft breaches used stolen or weak credentials,**
- **25 percent involved phishing**
- **Human error accounted for 22 percent." (Verizon Business 2020 Data Breach Investigations Report (2020 DBIR)**

Of course, as we all expected, things have gotten worse since the pandemic "The FBI's Internet Crime Complaint Center (IC3) was previously fielding 1,000 complaints a day. They are now receiving between 3,000-4,000". (Systems Engineering).

In addition, the FBI has issued report on Business Email Compromise, the FBI lists a series of things you can due to protect yourself from intrusion. Expressly, they direct you to **"set up two-factor or multi-factor authentication on any account that allows it and never disable it."** (FBI).

Smaller-Medium Size Businesses Specifically Targeted for Credential Theft

Small to medium-sized companies frequently have limited security in place. This makes them much more susceptible and attractive to malicious people.

The Verizon 2020 DBIR also reports that:

- **"Phishing is the biggest threat for small organizations, accounting for over 30 percent of breaches. This is followed by the use of stolen credentials (27 percent) and password dumpers (16 percent).**
- **Attackers targeted credentials, personal data and other internal business-related data such as medical records, internal secrets or payment information.**
- **Over 20 percent of attacks were against web applications and involved the use of stolen credentials."**

As bad as the statistics above show, System Engineering reports that since the beginning of 2020:

- **“There has been a 72% increase in cybercriminals trying to penetrate office networks and steal corporate data. (Source: ABC)**
- **Almost half of businesses have suffered a data breach or cybersecurity event as a result of the quick shift to the work-from-home model. (Source: Dark Reading)**
- **About 75% of businesses transitioned to remote work, in which 51% have seen an increase in email phishing and social engineering attacks. (Source: Barracuda)**
- **Of the 51%, 63% experienced a data breach. (Source: Kaspersky)**
- **The pandemic has led to a 37% jump in mobile phishing attacks. (Source: TechRepublic)”.**

New Technology Makes Credential Theft Easy

Why the rapid growth in cybercrime? It’s because there is new technology used by hackers and other cybercriminals that allows them to methodically reveal passwords. Passwords no longer need to be stolen and guessing passwords is no longer random. Known as a Brute Force Attack it makes even the most sophisticated password-only systems obsolete. These types of attacks are efficient at making small to medium-sized businesses even more susceptible to cybercrime.

Fortunately, the solution is MFA.

How Is MFA Implemented?

The facts are: passwords are easily stolen, email is the weakest link to cybercrime and MFA is the solution.

Therefore, email and application providers such as Microsoft, Google and Facebook have become obligated to include MFA as part of their security settings. However, these MFAs do not protect all systems. MFA must be enabled for each application or system that has one and a third-party MFA needs to be used for complete MFA implementation.

In the case of businesses, you typically need a network administrator to enable MFA for the entire company, as with the enterprise edition of Microsoft Office 365. On a personnel level, you will need to create policies and procedures for employees to turn on MFA for apps they use such as Facebook, particularly on any BYOD devices and which third-party MFA application to install.

Since MFA requires an additional credential to login, MFA requires a change to your login procedures. For example, when setting up an MFA, you may choose to have the user enter a verification code they received on their smartphone. Likewise, certain MFA methods can be setup to receive answers to security questions, thumbprint scans and more.

MFA solutions can also incorporate behavioral analysis for advanced, additional security. Known as “adaptive authentication”, it incorporates the setting or behavior of a user. For example:

- **What device is being used, such as a user’s smartphone, tablet, or a laptop?**
- **Where is a user is trying to obtain access, such as the home, a coffeeshop or office?**
- **When or what time of day a user is trying to access, such as late at night or during typical workday hours?**

Adaptive authentication both verifies a user and flags suspicious logins. In this case, the system will ask for additional credentials such as a verification code sent as a message to the user’s phone. This is particularly useful for that appear out of the ordinary. This is particularly useful for controlling the environment where a user can safely login.

Additional Tools Are Needed:

Just as with any security system included within a particular enterprise-level solution, you should also use a third-party application for full protection.

For MFA in particularly it is essential to have a third-party tool:

1. **First, other than the large organizations, most systems and apps do not include MFA as of yet.**
2. **Second, a third-party MFA can include additional features that are more in-line with your particular organization's needs such as the use of adaptive authentication.**
3. **Third, certain MFA tools can simplify multiple MFAs into a singular login making MFA easier to use across a multitude of systems.**

When looking to implement MFA for your business, we at Concensus recommend the following enterprise-level, third-party MFA tools for your consideration. You can read more about each tool in our blog What You Need To Know About Implementing Multi-Factor Authentication.

Identity Automation's RapidIdentity MFA This MFA tool provides additional protection across all access entry points including, offline desktops, both on-premise and cloud applications, portals, VPN, and more. You can choose which MFA is actually needed for your business and users can choose from a variety of authentication methods.

MicroFocus's NetIQ Advanced Authentication Is a method of advanced authentication that enables organizations to tailor the security as necessary. It contains the framework you need to implement strong MFA required to meet regulatory, industry, and client forces.

In addition to the enterprise-level MFA tools above, here are the top MFA applications:

- **Duo Push** Available through the Duo Push app, Duo Push is both dependable and easy to use. It automatically prompts each login to be confirmed with a security key device or by using a built-in biometric authenticator, such as TouchID, via WebAuthn. Users can also confirm their identity using a secure passcode generated by a physical token, a mobile device, or a network administrator.

- **Google Authenticator and Microsoft Authenticator** The Google Authenticator provides enhanced security for Google accounts and likewise the Microsoft Authenticator provides enhanced security for Microsoft accounts. They both use a 2-Step Verification, by requiring a verification code sent directly to a mobile phone via text.

- **OneLogin Protect** Gives reliable, integrated MFA protection. It eliminates the need for people using various services to manage multiple authenticators on their iOS or Android mobile devices.

What to Do to Protect Your Business

Time is the essence to enhance your security through MFA but where do you begin?

Begin by contacting our team of cybersecurity specialists at Concensus. We are the experienced experts you can trust and depend to implement MFA and secure your business.

Here are just a few of the ways our team at Concensus can help:

- **Enable Native MFA –** Where MFA is part of a system or application, we can be the network administrator or support your current admin in setting up the included enterprise-level MFA features.

- **Assess, Recommend and Apply Third-Party Tools –** We can examine the needs of your particular business and determine which third-party tool is best for you and your team. We then can implement this tool throughout your organization.

- **Implement Adaptive MFA –** Based on your particular needs, we can also implement advanced and intelligent MFA for your protection.

- **Advise on Policies –** MFA, just as with any cybersecurity process, requires a set of acceptable use expectations for your employees, especially for work-from-home, BYOD and other access situations.

In addition to MFA, Concensus offers experienced IT managed services in ALL aspects of cybersecurity, including:

- **Implementing Security software –** to protect from viruses, malware, spam and more. At Concensus, we also maintain the security software to ensure that all patches are up-to-date and installed.

- **Continuous Monitoring –** Concensus provides 24/7/365 monitoring that your networks are safe, and all network cybersecurity measures are working.

- **Additional Email Security–** since email is the weakest link, we also provide managed IT services for

  - **Anti-Phishing Systems-** that reviews emails to see if the sender is valid, do not contain any links to a known malicious site and has the ability to send secure email.
  - **DNS protection Secure (Domain Name Systems) -** DNS protection is when your email spam/anti-virus solution does not catch a malicious email. It tracks known malicious sites and blocks access to that site and contains a web filter to block sites by category (gambling, drugs, etc).

- **Awareness, Training and Testing -** At Concensus, we can guide you on the best Security Awareness Training (SAT) service to educate your employees on passwords, email security, website security, and physical security. Training your employees also increases your eligibility for cyber insurance.

- **How to Report Breaches and Create an Incident Response Plans** –Mistakes happen. Since everyone and every organization is vulnerable, we can help create the plan, lead should an incident occur, and assist in remedying the situation.

- **Backup and Recovery Policies and Plans –** At Concensus we apply the right technology so you have confidence in your working, secure and tested backups and recovery.

- **Cyber Insurance –** The team at Concensus are experts in the matter of cyber insurance including requirements for compliance such as cybersecurity policies, employee security training, and auditing of security technologies, all being maintained and updated.

- **Most Importantly, We Support –** At Concensus we are here to support and secure you, your business, and your data. We also assist with any issues and guide you through both the business and technological aspects of cybersecurity protection.

Our team of experienced IT experts at Concensus is here to be your trusted partner and protector. **Contact us, today.**

Sources:

- https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report
- Coronavirus pandemic creates ‘perfect storm’ for cybercriminals to exploit people working from home: Experts - ABC News (go.com)
- Half of Companies Have Suffered a Cybersecurity ... (darkreading.com)

CONCENSUS
TECHNOLOGIES

51 DUTILH ROAD, SUITE 140
CRANBERRY TOWNSHIP, PA 16066