Inversion6

PROTECT YOUR ORGANIZATION WITH OFFICE 365 SECURITY SOLUTIONS

HOW TO USE THE SECURITY TOOLS AVAILABLE TO YOU TO PREVENT BREACHES, HACKING, PHISHING, AND MORE

Jack Nichelson | Jason Middaugh

CONTENTS

MORE THAN 200 MILLION USERS...

...and Just as Many Risks

Microsoft Office 365 is among the most widely used SaaS products in the world. With more than 200 million active users, the Office 365 cloud houses a staggering amount of data that grows larger and larger by the minute as organizations store emails, user information, and documents for quick, convenient, and collaborative access.

As a security-minded company, Microsoft invests **more than $1 billion** on cybersecurity research annually and announces security updates to Office 365 on a frequent basis. These measures make Office 365 a relatively secure choice for organizations around the world, but cyber attacks are still an unfortunate reality. An increasing number of data breaches continue to occur each year.

Stolen identities are among the most common means of unauthorized access to company Office 365 accounts, accounting for more than 80 percent of data breaches.

Once a user identity has been stolen, hackers can access a network from anywhere in the world, preying on vulnerable data and wreaking havoc within the system. In many cases, security risks come from unsafe practices or negligence within an organization rather than inherent vulnerabilities in the product. It's important to employ best practices in accordance with usage guidelines of the Office 365 platform to ensure minimal risk to sensitive data.

One key vulnerability to any system comes from weak login credentials, which are easy to steal or hack. Auto-generated usernames that mimic employee names tend to be standardized across companies and are particularly vulnerable when paired with prototypical passwords that some employees may never change.

Even strong login credentials can fall victim to phishing scams, which trick users into supplying login credentials so that hackers can access sensitive information. One such phishing scam involves a fake login page, created by hackers and embedded where users might access it, that tricks employees into giving away their credentials. Another involves phone calls or emails from hackers posing as company tech support, requesting login information to perform restorative or maintenance work.

Microsoft is aware of the risks posed by stolen login identities and has taken steps to address them. However, not all administrators are aware of the options available to help prevent a data breach. By employing multi-factor authentication, conditional access, modern authentication, and the use of security risk mitigation programs like **Secure Source**, as well as limiting access by legacy protocols, administrators can reduce their vulnerability.

Let's take a look at each of these and how they can help your organization stay safe.

MULTI-FACTOR AUTHENTICATION

What is Multi-Factor Authentication?

Multi-factor authentication is a basic, effective solution to the vulnerability inherent within a security system that relies only on username and password combinations to protect a network. When a network only requires these two pieces of information to give users access, it's allowing anyone who knows that information, may have stolen it from the employee, or may be able to generate the combination to access the network.

This is an incredibly non-secure practice, as people often cannot remember this combination. The average person has 191 passwords for a variety of accounts and needs — so remembering a complex, unique, or otherwise different password for a work account is next to impossible. Employees that use the same passwords for most of their online life also put your network at risk should their login information be stolen elsewhere. Multi-factor authentication helps to address this problem.

How Multi-Factor Authentication Works

Multi-factor authentication, as the name implies, requires users to prove their identity before accessing the company's network or being able to view and use sensitive company information. This provides additional security beyond conventional login credentials. The multi-factor authentication process verifies user identity by confirming access with an outside device associated with the account — typically a mobile device.

Within Office 365, several options for multi-factor authentication are available at no additional cost. Administrators have the option to require two or more of the following in addition to conventional login information:

- A randomly generated passcode
- A phone call
- A virtual or physical smartcard
- A biometric device

With this process in place, companies will be in a better position to protect critical information and their network as a whole. Even if you already have a password protection or storage system in place, multi-factor authentication will help provide an additional layer of security and peace of mind. And considering the potential damage hackers and cybercriminals can inflict on companies (to the point of forcing operations to cease), requiring your employees to take an extra 30-second to oneminute step is worth it.

Even if you already have a password protection or storage system in place, multi-factor authentication will help provide an additional layer of security and peace of mind.

Additionally, remember that multi-factor authentication is a free service offered as part of your Office 365 subscription. Other services are available that provide enhanced security above and beyond the base level multi-factor authentication option. Examples include Okta, an adaptable identity and access management solution that secures all workforce and customer identities everywhere: cloud, hybrid, and on premises.

PHISING AND SPAM PREVENTION

What are Phishing and Spam?

By now, you're likely somewhat familiar with what **phishing** is — and you most certainly know what **spam** is. And while Office 365 offers a variety of free, readily available solutions to help prevent these two threats, they may not be the only thing your business needs to keep employees and data safe.

Phishing and spam are both the use of deceptive tactics to acquire sensitive information, ranging from consumer data and logins to financial or personal information that you otherwise wouldn't share.

Phising scams are elaborate and more targeted than spam, ranging well beyond just emails to include websites and pages built to resemble those employees might normally visit.

Even the URL structure on the fake page might be similar, but to those who aren't paying attention, minor differences won't be enough to prevent an accidental form completion or login.

Education is the First Step

Most organizations will educate their employees and customers about potential phishing scams, but it's critical that anti-phishing and spam education be an ongoing, consistent effort. Employees leave and join companies every day. New employees need to be trained on what to watch for with respect to your business, and employees that leave take their knowledge and experience with them. That's why ongoing education is critical to ensure that employees are ready.

Make Use of Office 365 Options

Office 365 already comes with anti-phishing support that should be used as a first line of defense. ATP anti-phishing is available in the Security & Compliance Center in your Office 365 environment. These tools use a set of machine learning models along with algorithms that detect impersonation attempts on incoming messages to protect against phishing attacks. And while they're a great first step, you will likely need additional support.

Work with Specialized Service Providers

While an internal IT and security team, along with ongoing education, can certainly help to build the foundation for phishing support, it's not entirely enough. Consider working with expert solutions providers such as Mimecast or Proofpoint can help add that extra layer of protection on top of existing efforts. Inversion6® works with these companies and can assist you in setting them up to get additional protection for your employees and organization.

CONDITIONAL ACCESS

What is Conditional Access?

Conditional access is a method of security that controls which devices and users have access to services and data sources within an Office 365 environment. Through this process, administrators can create a list of criteria through which network access can be allowed or denied that is completely separate from standard login information.

How Does Conditional Access Work?

Conditional access criteria can be any specific features the administrator chooses. These most often focus on the location of a user attempting to log in, the device from which that user is working, the application they are using, or a history of suspicious login activity associated with a particular account.

▪ **Location-based Conditional Access** — Restricts access to a network based on the geolocation associated with the device or IP address from which a login is attempted. This kind of restriction can prioritize corporate locations as trusted logins while limiting access from specific locations or identifying rapid changes in login locations as suspicious.

▪ **Device-Based Conditional Access** — Prevents devices that don't meet administrators' security standards for accessing a network. Within these settings, administrators can specify allowable criteria that grant access either strictly to devices managed by the company or to a wider array of options that meet the given security criteria.

▪ **Application-Based Conditional Access** — Focuses on information at a more granular level, restricting access based on the application that a user is accessing the network from when on a personal or mobile device. In this way, application-based conditional access keeps data safe and employees productive, even when they have to work from locations and devices not associated with company locations or equipment.

▪ **Risk-Based Conditional Access** — Uses machine learning to identify suspicious login behavior based on established norms for a given account. If a login attempt falls outside of normal patterns, additional authentication can be required to keep the account secure. Risk-based conditional access, like location-based conditional access, also tracks real-world locations to identify impossible location jumps or unlikely points of access based on an account's history.

SECURE SCORE MONTHLY

What is Secure Score Monthly?

Office 365 also offers access to **Secure Score**, a security management service that works to identify strengths and weaknesses in existing security protocols. It does so by comparing the security practices of a company to an industry baseline, calculated by compiling best practices by industry users of the specific Office 365 services used by the client.

How Does Secure Score Work?

Scores are expressed as fractions. The denominator represents the sum of all industry baselines for security controls, and the numerator represents the sum of all the security controls currently used by the client themselves.

For example, a client may receive a Secure Score of 54/421. In this case, the client has used some security protocols, earning a total of 54 points, but best practices for the products the company is using indicate that they should be using more to achieve a higher score. The maximum security in accordance with best practices should be a total of 421 points.

In situations like this, where a client is not making maximum use of the security products available to them, Secure Score recommends actions along with associated point values to raise the score. These actions are also ranked in terms of cost and user impact to help clients prioritize essential and cost-effective actions.

Using Secure Score, you can make more effective use of Office 365's built-in security features to improve your overall security standing. Often, companies aren't aware that these features are available with the products they've purchased, but Secure Score will notify you of updates and actions that you can take and where they are.

And according to Microsoft, organizations that are using Secure Score have seen their scores increase five times more than organizations that aren't using it. Needless to say, Secure Score is a great way to gain a high-level view of your overall security performance based on your environment and how you can take steps to improve it.

Organizations that are using Secure Score have seen their scores increase five times more than organizations that aren't using it.

One great place to get started is with the **CIS Microsoft 365 Foundations Benchmark report**. It's a great (free) guide to follow for turning on security settings. In particular, see page 125 and use the checklist as a tool to work through the recommendations. Track your updates and take screenshots to document your work.

LEGACY PROTOCOLS

What is a Legacy Protocol?

Many organizations' IT administrators do not realize that their company networks are vulnerable to access through **legacy protocols** — dated networks that are not part of the TCP/IP protocol suite but can still allow access into protected data. POP3, IMAP, and ActiveSync are legacy protocols common to Office365 but they can be disabled for individual users to increase security.

While legacy protocols can enable greater access to cloud-based apps within your network, the challenge is that they don't support multi-factor authentication. This becomes a balance between usefulness and security, and in our opinion, the latter should always take precedence. However, sometimes legacy systems still need access. That said, legacy protocols have been the targets of recent security incidents — meaning the risk involved in using them is quite real and not something to be left to chance.

Legacy protocols have been the targets of recent security incidents - meaning the risk involved in using them is real.

Additionally, the proliferation of mobile devices within organizations' workforces (such as those adopting BYOD or COPE policies) presents another security challenge for IT teams. Companies still using legacy protocols like ActiveSync should consider enabling a device quarantine to ensure that not just any device can gain access to the network.

Striking the Right Balance

Multi-factor authentication should be absolute within your organization. It helps protect your network from hackers and other breaches by adding another level of verification on top of existing login credentials. However, you may have certain users that still need to access the network using legacy protocols.

In this instance, one recommendation is to block legacy protocols using a conditional access policy. This way, you can set permissions for users with legacy protocols and block them for everyone else. Note that conditional access is only enforced after the first level of authentication is complete, so conditional access in this sense cannot and should not be used or considered as the first line of defense. It's simply a method of narrowing who can have access to the network using a legacy protocol.

ACHIEVING MODERN AUTHENTICATION

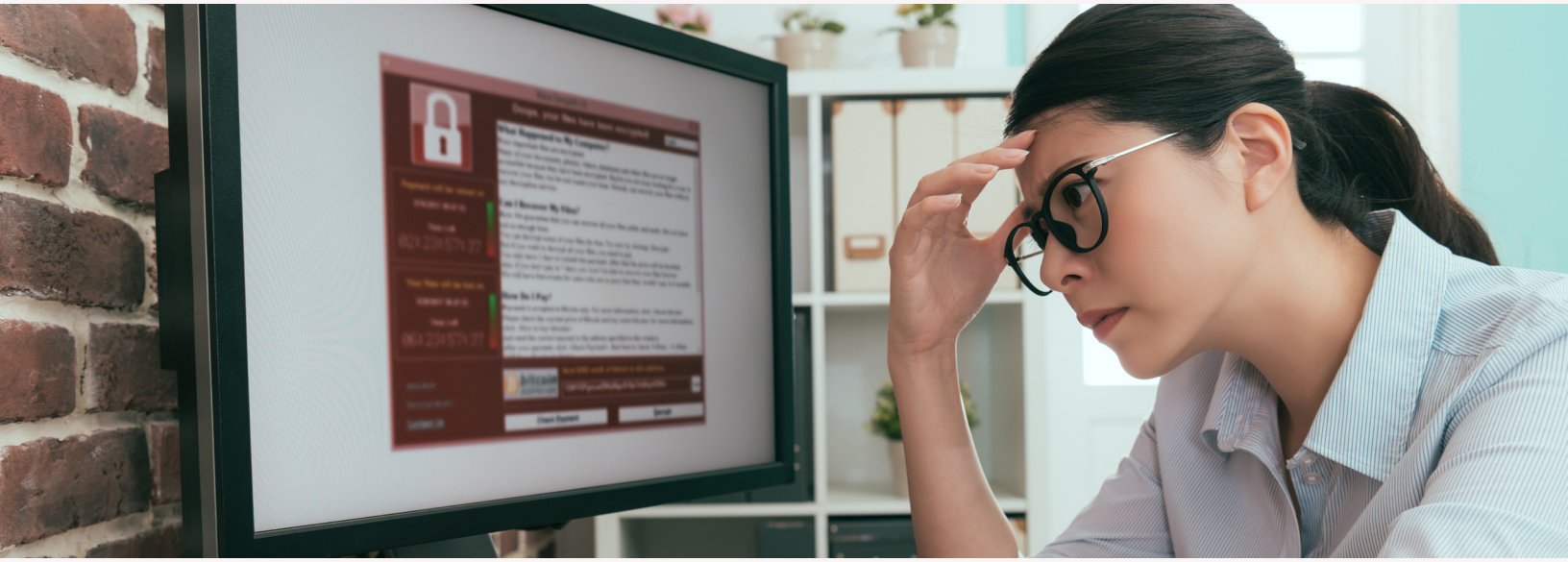
What is Modern Authentication?

The use of **modern authentication** can also help protect against security breaches. Modern authentication is the term used by Microsoft to refer to the combination of security measures — like conditional access — and authentication and authorization methods, such as multi-factor authentication.

With modern authentication enabled, organizations can sign in securely through an Active Directory Authentication Library (ADAL) — allowing protected logins and secure remote access while also eliminating the need for employees to continuously re-enter login credentials.

Modern authentication keeps employees productive throughout the day while minimizing the risk of your network being exposed.

By default, modern authentication is enabled for all users. The platform continues to verify your employees as they use your systems, but the story of how they access everything changes on the back-end. Modern authentication is dependent on the systems and applications you're using and what your overall network looks like, so it's worth considering how your employees use systems throughout the day and what your access levels should look like to ensure it's properly set up.



ADDITIONAL SECURITY CONSIDERATIONS

Mainstream Support

Mainstream support refers to the amount of time that Microsoft will continue to support its existing systems. For example, Microsoft Office 2019 — a standalone purchase that included common applications — currently allows connections to Office 365. Because of this, Office 2019 is still under mainstream support until October 2023. While Microsoft will still continue to release security-related fixes, any non-security-related issues won't be fixed. Over time, the quality of the connection will diminish, necessitating a transition from Office 2019 to Office 365. The longer an organization continues to use older suites like Office 2019 and others, the riskier it becomes for them to connect to 365.

The longer an organization continues to use older suites like Office 2019 and others, the riskier it becomes for them to connect to 365.

Office 365 Data Preservation

A key aspect of Office 365 is its ability to instantly save your data. While this is helpful for immediate needs, the situation changes long-term. There is no redundancy or failover for old data. If a user or admin were to accidentally delete a message or file (whether intentionally or unintentionally), it will likely be gone and irretrievable after 90 days. There is the option to recover it up to that point, but if you want to preserve information long-term, you'll need a separate backup or archiving solution. Be sure to update your policies to reflect the appropriate amount of time you need for your data as well.

Mailbox Auditing

Mailbox auditing provides time-sensitive security information for users in the event that their email accounts were compromised. While this is now automatically enabled for new users, this wasn't always the case in the past. If someone were to access your account for malicious purposes, their first step is likely to set up forwarding. Mailbox auditing notifies you of settings adjustments like this as well as suspicious login attempts (whether they succeeded or not). Ensure your organization has this activated for its users.

Admin Account Segmentation

Global admin accounts are critical because they provide control and visibility into all other accounts. When this account is established, many users will tie their business account to this admin account. If those users were to be breached, the attacker would have access to the admin account and subsequently all other access they would need to wreak havoc.

Disabling Skype Federation

Skype has become a critical business communications tool for many organizations utilizing Office 365. However, Skype is set to be federated by default. This means people from other organizations can find users at your organization and send your users messages. Malicious users can pose as employees from your organization, making it easier for them to get the information they need such as passwords or other information because your employees thought they were chatting with a coworker. Ensure your organization's Skype settings are set to only allow federation with trusted partners.

External Subject Line Tagging

Last but not least is a common best practice that far too many organizations have yet to fully adopt. Tagging the subject lines of emails sent from outside the organization with an "EXTERNAL" modifier helps to immediately communicate to your employees that the message did not originate from within your secure network. This tells employees to approach the email with caution and to watch for suspicious links, attachments, etc.

TRUST SECURITY TO THE EXPERTS

Strong Security Starts with a Strong Strategy

Managing information security — particularly when using Office 365 and other broad productivity suites — is a complex challenge, which can have serious consequences for any organization when handled improperly. Security programs are highly context-specific and should be developed and maintained by someone who has familiarity with an organization's specific needs to avoid catastrophic data breaches — or wasted resources on threats that are unlikely to manifest. This is why many organizations use and are often required to have a Chief Information Security Officer (CISO). This position assumes overall strategic responsibility for the tech security of an organization.

Security programs are highly context-specific and should be developed and maintained by someone who has familiarity with an organization's specific needs.

What Do CISOs Do?

CISOs use their expertise to develop security strategy, execute specific security-minded projects, advise administrators on ongoing security developments, and mentor teams on best practices related to cybersecurity. CISOs work with IT and other departments to ensure that the organization's overall security strategy is built, updated, and followed.

However, many organizations find employing a full-time, in-house CISO to be financially or practically unsustainable. The position requires more than just IT and security experience, but also strong leadership, top-of-the-line communication skills, and relationship building.

To help companies take advantage of the CISO position without having to navigate a complex recruitment process, Inversion6® offers CISO services to organizations that want a locallybased, experienced cybersecurity executive who can develop a security plan to meet their unique needs. Our CISOs are security veterans who get to know the members of each organizational team and work collaboratively to understand their infrastructure and IT setup. With this knowledge, they collaborate with the entire Inversion6® staff to create security practices that are uniquely suited to meet the organization's needs in perpetuity.

Put Our Expertise to Use for Your Business

These practices can and should involve successful navigation and implementation of the resources available to enhance the security surrounding Office 365 to prevent data breaches associated with stolen user identities.

ABOUT INVERSION6®

Inversion6® provides customized security solutions to support your internal security efforts. Whether you're looking for CISO, MSSP, or security software guidance, Inversion6® partners with you to keep your company safe. Dedicated to long-term service, Inversion6® will work to protect your organization relentlessly — every hour of every day — by investigating and detecting potential threats, then communicating those concerns and finally by eliminating security issues.

With an entire suite of services and programs, we provide a managed security solution that will monitor and resolve information security threats around the clock to add a new level of protection for your organization.

With our innovative CISO for Hire platform, we partner clients with high-level information security executives to manage and guide your security needs and responses alongside your own team. We also offer network solutions, forward-thinking security measures, and dedicated storage solutions as part of the breadth and width of services and products we provide.

Get in touch

216.535.4100 info@inversion6.com

ABOUT INVERSION6® CISO SECURITY SERVICES

Let Us Own Your Security Problems

Less expensive and easier to retain than hiring top talent in-house, Inversion6® CISOs are responsible for delivering on projects, moving the needle on security, and being readily available to your team in times of crisis. We don't utilize junior level staff consultants — only security veterans with decades of real-world expertise in the security industry.

How It Works

What We Offer

▪ **CISO FOR HIRE** — Our CISO becomes an ongoing part of your team responsible for developing security strategy, executing on projects, advising you on the latest security developments, and helping to mentor your team on security.

▪ **MANAGED SECURITY SERVICES** — Our team can monitor your security 24/7/365 through a combination of tracking solutions as well as our expert security team. Behaviors and anomalies are identified early to help identify and prevent incidents.

▪ **THREAT INTELLIGENCE PROGRAM** — We help you develop an entire program tailored to your needs and resources. Inversion6® will train your team on intelligence gathering, create Indicator of Compromise (IoC) triggers, and develop program deliverables.

▪ **SECURITY OPERATIONS ASSESSMENT** — Have one or more security tools but no documented process to use them? Our security operations assessment takes an enterprise-wide review of your existing security operations.

▪ **RISK ASSESSMENT** — We take an enterprise-wide look at your security practices and provide a strategic assessment and scorecard of how you stack up. You receive a heatmap of identified risks and a complete security plan prepared by our team.

▪ **TAILORED SOLUTIONS** — If you have something unusual, something that doesn't seem to fit a cookie-cutter consulting engagement, or simply a problem that you've not been able to solve, our team would love to help.

Get a free consultation from an Inversion6® CISO at Inversion6.com