FINCHLOOM

Microsoft 365

MODERN WORKPLACE

Into the era of secure remote work

A business guide to cloud security for the new remote workplace

Business opportunities and security risks associated with the rapid shift to remote work

Something many small and medium-sized businesses have discovered during the rapid shift to remote everything: There's a lot to be gained by not relying on a physical space. It can save overhead, reduce travel expense, and some studies have found it has increased worker productivity (one found a 13% performance boost among at-home workers).[1] As a result, many businesses are seriously considering tools and strategies to make the non-physical workplace a permanent part of their businesses.

To succeed, this transformation of physical businesses will require new structures and processes, especially for smaller businesses that were not used to working remotely. Regardless of size, all companies now need to think about securing remote endpoints and IT resources. Employees need to be more vigilant than ever. Cyberattackers have made it clear they're not taking any time off.

Many of us saw the additional security risks of the remote work explosion. Video data breaches represent only the visible fraction of other, less flamboyant, but more costly threats enabled by the new scale of endpoint devices in use. Just during the first quarter of 2020, COVID-19 opened up a floodgate of new data security threats, including:

- **220x increase** in spam from February to March of 2020
- That increase includes **907,000 spam messages** related to COVID-19
- **737 malware attacks** that leveraged the crisis
- **A 260% increase** in malicious URL hits in February and March 2020[2]

And that's only in the United States. Bad actors aren't slowing down, so you, your IT teams, and end users all need to be ready now for the increased security risks in this new age.

[1] "Remote Working: The New Normal?" Casey Rue, Forbes, May 20, 2020.

[2] Trend Micro research data based on coverage of their Smart Protection Network, Jan. 1 – Mar. 30, 2020.

A two-part security challenge: Volume and security

Like so many other companies making the decision to shift to remote everything, your company's first challenge was how to ensure unimpeded performance for your remote workers who are trying to access their tools and data—or just find a reliable internet connection.

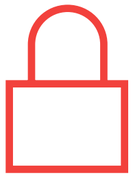
Following close on this first issue is the question of security. Suddenly it's the ultimate bring-your-own-device (BYOD) world. Every employee is now remote and focused more on productivity than on following strict security measures, no matter how essential they may be. They'll access the data they need however they can; often bypassing VPNs to access cloud services or grabbing hotspots wherever they can—secured or not. This do-it-yourself attitude can lead to risky activities beyond your control, such as employees downloading software on their own.

With everyone using whatever devices are handy—personal phones, home computers, even kids' tablets (it has happened!)—the situation is especially perilous. One wrong click can instantly launch an attack that could jeopardize your entire business.

Given the limited capabilities of traditional perimeter firewall and VPN solutions to protect against these remote threats, companies need new security measures, new levels of expertise, and new technologies to protect their assets. The good news is you can build on current measures to get there.

Time is not on your side: Get a handle on your security picture

If you haven't had time to perform basic endpoint hygiene and connectivity performance checks on your computers and devices, better late than never. In addition to confirming all your devices have the necessary endpoint protection configurations for all this new off-LAN activity, ensure your employees are following recommended security practices by asking these three important questions:



1. Have you reviewed and adjusted the security settings of your cloud tenant and your organization's internal network?

2. Have you made sure the security settings and measures for remote users are appropriate for current and foreseeable levels of usage?

3. Is your team proficient in all the latest security threats or do they require assistance?

FINCHLOOM Microsoft 365

Make remote workers the center of attention

Remote workers are now the core of your productivity. The devices they work on can no longer exist at the edge of your security planning; they are dead center and must be treated as such starting now. All that mixing and matching of personal devices with company equipment demands different practices and elevated controls. That means much more than the basic antivirus and antispyware protection, including multi-factor authentication (MFA), onboard endpoint detection, and response (EDR) capabilities.

Not only should your remote workers be aware of these new measures, but the tools and safeguards you use to attain and remain at a new level of endpoint and data security should meet those needs.

With the world rapidly—and permanently—changing, now is the time to enlist the help of a partner that has already worked out the best practices to face it. Without this critical help, you can't be sure each endpoint requesting access to internal resources meets security policy requirements. You need the right tools to track and enforce policy on all devices and with employees everywhere, while delivering easy user onboarding and offboarding.

We can help.

FINCHLOOM Microsoft 365

Equip your organization with reliable phishing prevention

How Finchloom's PhishPrevent provides a unique advantage

Phishing attacks result in unprecedented loss of time and money. PhishPrevent, Finchloom's managed **email and identity protection service**, helps ensure phishing attacks do not gain access to your organization's data and information. Threats are not only identified quickly—they are reviewed and addressed immediately by a team of real people. Any emails from unknown senders that appear malicious are automatically marked with a warning banner and can be easily reported with an Outlook-integrated "PhishPrevent Report Button." Emails that pose threats are not only removed from the inbox of the employee who reported them—but also from the inboxes of all employees who received the email.

FINCHLOOM Microsoft 365

How PhishPrevent empowers Outlook—and employees

An exclusive, managed security solution for Microsoft 365

Finchloom is a 100% Microsoft Partner and modern, cloud-only company. Unlike traditional CSPs that manage outdated servers, Finchloom is focused on transforming and moving customers to the cloud.

PhishPrevent merges different technologies with established methodologies specific to Microsoft. The result is advanced protection for organizations against a variety of threats—including email, identity, and domain name phishing. PhishPrevent is also unique because it doesn't just identify and eliminate threats—it empowers employees to do the same by providing live and on-demand video training, e-mail awareness campaigns, and regular phishing simulations.

FINCHLOOM Microsoft 365

Enhanced security responses for the new remote work environment

The decentralization of the workplace makes endpoint security more critical than ever. New tactics used by malicious actors require focus on different tools and solutions. If your organization uses Windows 10, **odds are you already have access to the world-class antivirus and antimalware solution already built into the operating system.** You also probably have the cloud license to activate centralized management and the greater capabilities of Microsoft Defender.

Microsoft Defender for Endpoint gives you unmatched breach remediation and research capabilities. With a graphical representation, this tool enables security teams to map the precise point at which an attacker entered your network, how the attacker moved once inside, and the activities they engaged in.

It is one thing to remediate a network breach but having the rich details of exactly how the breach occurred enables you to make sure any vulnerabilities in the network are found and corrected to prevent future breaches.

Here are three ways we can help you immediately leverage your current Microsoft Defender technologies to face security challenges now and in the future:

Three ways to enhance security now

1. Phishing: Be the one that got away

Social engineering has always been a successful vector for malicious actors. Now with more employees working on their own, the bad guys have more targets of opportunity. With cloud providers hardening their security more than ever, phishing for credentials and spoofable material is becoming a path of least resistance. Once they have convinced a user to give up their sign-in information, hackers can accurately spoof the emails of internal users. The user receives an internal email, clicks on the link and that's it. The links lead to websites that look very real. For example, they might mimic the Microsoft Office 365 sign-in page. When a user enters credentials on this site to sign in, the bad actor then has access to your environment for further attacks.

Phishing is successful because even with the proper training, anyone can be fooled. Training must be regularly performed and reinforced through simulated activities—just like fire drills—to remind users to be skeptical of any email they receive.

If a single phishing attack gets through, it can cost your organization hundreds of thousands of dollars and a reputation damaged beyond repair. Just look at the news in the last several years. For training that's unmatched, as part of the PhishPrevent managed service, Attack Simulator for Office 365 helps users defend themselves and your company using the Microsoft Intelligent Security Graph. It's constantly learning from global signals received from one of the largest telemetry systems on the planet.

For example, Microsoft Office 365 scans 400 billion emails every month and finds a large number of malicious spear-phishing emails. The Attack Simulator carefully crafts simulated spear-phishing emails based on this real data, ensuring the most realistic attack experience for your user population. It then tracks and reports on user responses to the simulated email security events, providing invaluable data on how to better secure the organization.

Three ways to enhance security now (continued)

2. Watch out for well-intentioned “shadow IT”

As we’ve said, the new remote world of work is full of bright end users. They’re bound to think they have better tools than those your IT department authorizes. And they will use them. Sometimes a tool can go internally viral, becoming the app-of-choice before IT can stop it, or even become aware of its existence. Though your users see these as smart and cool new solutions, and see themselves as taking initiative to deploy them, they’re dangerous to your data security and can obviously become the source of network breaches. We can help you through our managed security service to continuously monitor for these unsanctioned applications and the “shadow IT” they engender.

3. Keep your defenses strong

We can help. Your known tools can help protect you from unknown new threats—if you know how to use them. Our team of security experts will help ensure that your company’s critical data protection is innovative enough to stay ahead of the threat environment with tactics that include:

- Security alert monitoring of Office 365 with Security Score
- Baiting and trapping of threats using honey pots
- Setup of antivirus active threat monitoring and mitigation
- App installation monitoring to prevent “shadow IT” behaviors with Device Guard
- User data classification setup
- Simulations of email phishing attacks raising awareness
- Simulated password spray and brute force password attacks to better secure credentials

Jordano’s enhances Outlook security with trusted Microsoft partner

Jordano’s IT department needed to provide additional security and mail protection for the company’s Microsoft 365 users. Finchloom's PhishPrevent was selected as the turnkey, managed service to apply security best practices, user training, and ongoing support for email and identity for Microsoft 365.

Description

For over 100 years, Jordano's has been a food and beverage distribution powerhouse in central California.

Challenge

With employees working in the office and from home, Jordano’s needed a way to protect their employees’ email and identity while providing them with secure remote access. Executive management wanted to provide employees with an additional tool to combat phishing and prevent business email compromise.

Solution

Because Jordano's was already a Microsoft 365 Business Premium subscriber with email migrated to Exchange Online, it was easy for Finchloom to implement PhishPrevent and start securing and managing email and identity threats. The process started by locking down their Microsoft 365 tenant, utilizing Azure AD, and applying security best practices such as multi-factor authentication. Finchloom then rolled out the "Report Phishing" button to all users in their Outlook client.

Results

PhishPrevent was a simple, easy to use, add-on service for Microsoft 365 delivered by a trusted Microsoft partner. Jordano’s IT staff members now receive monthly reports showing the number of attacks thwarted and the top activity in the organization related to suspicious behavior.

FINCHLOOM Microsoft 365

FINCHLOOM

Microsoft 365

Back your business with the power of PhishPrevent

Finchloom's team is ready to provide a complimentary demo and share how they can protect your business. Additionally, a free breach assessment and report is available to Outlook users.

LEARN MORE