technology times

Prevent phishing attacks with these Microsoft 365 Defender features

What is proactive cybersecurity, and how do you implement it?

Internet bandwidth requirements for remote workers

Surf securely with a VPN

Velocity Technology

Velocity Dark Web Monitoring Service

Billions of email/username and password combinations have now been captured by hackers and are being sold on dark web marketplaces. This service reports what breaches have occurred that contain an email address or username tied with your email domain and if included in the data, the password that accompanied it.

Velocity will monitor your email domain and send you a monthly report similar to that shown below:

Take action to ensure that your company email addresses and passwords are not being sold on the dark web.

Contact us today for a quote on this service so you can avoid having your company's email accounts being used by cyber criminals for payment scams and other fraudulent activities.

Prevent phishing attacks with these Microsoft 365 Defender features

Microsoft is a provider of powerful and intuitive tools that improve efficiency, productivity, and security. And as phishing attacks become more sophisticated and prevalent, Microsoft is taking steps to protect its users, one of which is releasing powerful cybersecurity tools via Microsoft 365 Defender. Here are some of them.

1. Anti-phishing
The most dangerous types of phishing scams involve emails that are disguised to appear like it's from an entity. An attacker may use cunning tactics, such as referring to the victims by their nickname. They may even take over actual email accounts and use these to trick their victims.

Through machine learning, Defender creates a list of contacts that users normally communicate with. It then employs an array of tools, including standard anti-malware solutions, to differentiate acceptable from suspicious behaviors.

2. Anti-spam
Since common phishing campaigns utilize spam emails to victimize people, blocking spam is a great way to protect your company from such attacks.

Defender's anti-spam technology addresses the issue by examining both an email's source and its contents. If an email is found to come from an untrustworthy source or has suspicious contents, it is automatically sent to the Spam folder. What's more, this feature regularly checks the activity of people in your company to ensure that none of them sends out spam emails.

3. Anti-malware
Malware, such as ransomware and spyware, can spread via phishing emails. Ransomware locks systems and files from users until a ransom is paid. Spyware, on the other hand, steals data by recording keystrokes, copying clipboards, and taking screenshots, among other methods.

Defender employs a multilayered defense against both known and unknown types of malware. This covers the different stages of email transmission security, including filtering potentially harmful attachments, and real-time threat response. Microsoft also regularly deploys new definition updates to keep its defenses armed against the latest threats.

4. Sandbox
It's not uncommon for some users to accidentally open a malicious email attachment, especially if they're not careful.

Defender resolves this issue by opening all attachments in a sandbox first. This sandbox is an isolated environment, so if the attachment is malicious, it will only infect the sandbox and not your actual system. Microsoft will then warn you not to open the file. If it's safe, you will be able to open it normally.

5. Safe Links
Instead of attachments, some phishing emails contain URLs that lead to fraudulent websites — often made to look like legitimate ones — that require victims to provide their personal information. Some of these URLs also lead to pages that download malware into a computer.

Through a process called URL detonation, Safe Links protects users by scanning the links in their emails and checking for malicious behavior, such as the transmission of malware. If the link opens a malicious website, Microsoft Defender will warn users not to visit it. Otherwise, users can open the destination URL normally. Even so, the service will rescan the link in the succeeding days and report any suspicious changes.

What's great about Safe Links is that it also scans links in emails from people within your company and works on files uploaded to Microsoft Teams and SharePoint.

6. User Submissions
Defender allows you to set a specific mailbox to send emails you deem a threat. The User Submissions feature lets you set criteria for both malicious and safe email and identify mailboxes besides your spam folder to keep these messages in. This feature gives your administrators greater control over which emails to flag and which to report to Microsoft.

7. Enhanced Filtering
If your company uses third-party services to route emails to your on-premises environment before they are sent to Microsoft 365, you will benefit from Enhanced Filtering for Connectors. Defender uses inbound connectors to determine the trustworthiness of email sources. The more complex your routing scenario is, the more likely that an email's inbound connectors will not reflect its real source.

Enhanced Filtering preserves authentication signals that may have been lost over the course of routing emails. This maximizes the effectiveness of Microsoft 365's overall filtering capabilities, helping it detect spam and phishing emails.

If you need an email service that promotes efficiency while protecting your business, we can deploy and manage Microsoft 365 for you. Call us today to get started.

Published with permission from TechAdvisory.org.

What is proactive cybersecurity, and how do you implement it?

To keep cyberthreats at bay, you need proactive cybersecurity solutions in your arsenal. They identify and contain threats before they wreak havoc on your systems and cause significant productivity and financial losses. Here's all you need to know about proactive cybersecurity and how to implement it.

What is proactive cybersecurity?
Traditional cybersecurity is reactive — your IT team or managed IT services provider (MSP) will be alerted of a cyberattack after it has happened, leaving them to alleviate the impacts. In contrast, proactive cybersecurity is preventative — it takes into account all potential threats and seeks to identify vulnerabilities so that they can be addressed before they lead to larger, downtime-causing issues.

Many organizations have adopted proactive cybersecurity measures along with reactive ones and are now reaping the benefits, including the ability to stay one step ahead of cyberthreats and improved data compliance.

How to implement proactive cybersecurity
In adopting a proactive approach to cybersecurity in your organization, you must follow these steps:

1. Understand the threats you're facing
Before you can work toward preventing cyberattacks, you must know exactly what you're up against. Seek the help of your in-house IT staff or MSP in identifying the types of attacks that are most common in your industry.

2. Reevaluate what it is you're protecting
Once you have a list of the biggest threats to your organization, you need to take stock of how each can damage the various components of your network. Map out every company device that connects to the internet, what type of data they have access to (regulated, mission-critical, low-importance, etc.), and what services are currently protecting those devices.

3. Choose proactive cybersecurity measures to put in place
Depending on the risks and assets uncovered in steps 1 and 2, your IT team or MSP may recommend any of the following measures:

Proactive measure	What it entails
Security awareness seminars for all internal stakeholders	Train everyone from the receptionist to the CEO about effective security practices such as password management, proper mobile device usage, and spam awareness.
Updated anti-malware software or cloud-based service	Protect your data and systems against the latest and most menacing malware.
Routine software patches andupgrades	Minimize the chances of leaving a backdoor to your network open.
Web filtering services	Blacklist dangerous and inappropriate sites for anyone on your network.
Perimeter defenses (e.g., intrusion prevention systems and hardware firewalls)	Scrutinize everything trying to sneak its way in through the borders of your network.

Policy of least privilege	Limit users' access only to the data they need to fulfill their tasks.
Data segmentation	Rank data according to sensitivity and build micro-perimeters around high-value datasets.
Full-disk encryption	Make data stored in computers and portable devices unreadable so that if these machines are stolen, the files they have inside remain secure.
Virtual private networks	Make data transmitted across unsecured connections unreadable so that intercepting it would become futile.
Strict access controls	Prevent unauthorized access to accounts by using strong passwords, multifactor authentication, and auto screen locks and logouts for idle users.
AI-powered network monitoring	Identify suspicious user and software behaviors such as employees accessing files outside their departments.

If you're looking to implement a proactive cybersecurity strategy to protect your business's critical systems, give our professionals a call today. We'll assess your needs and recommend the best, most effective solutions to address them.

Published with permission from TechAdvisory.org.

Follow us on LinkedIn

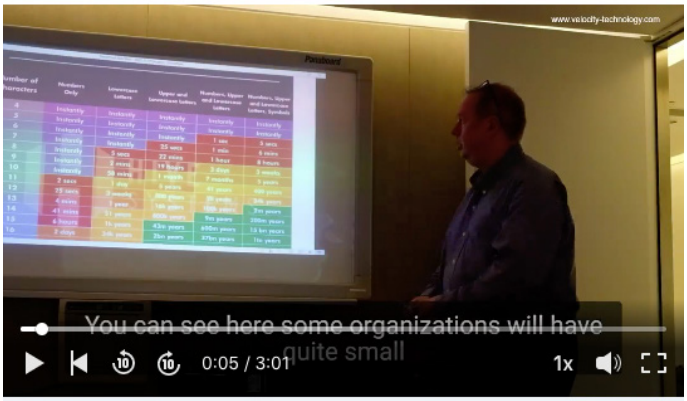
Velocity Technology Limited
242 followers
5d • Edited •

Is your password secure?

In this video, Stuart Sanders (Chief Technology and Security Officer at Velocity Technology Limited) shares why password length matters and why now is the time to think about your password strategy.

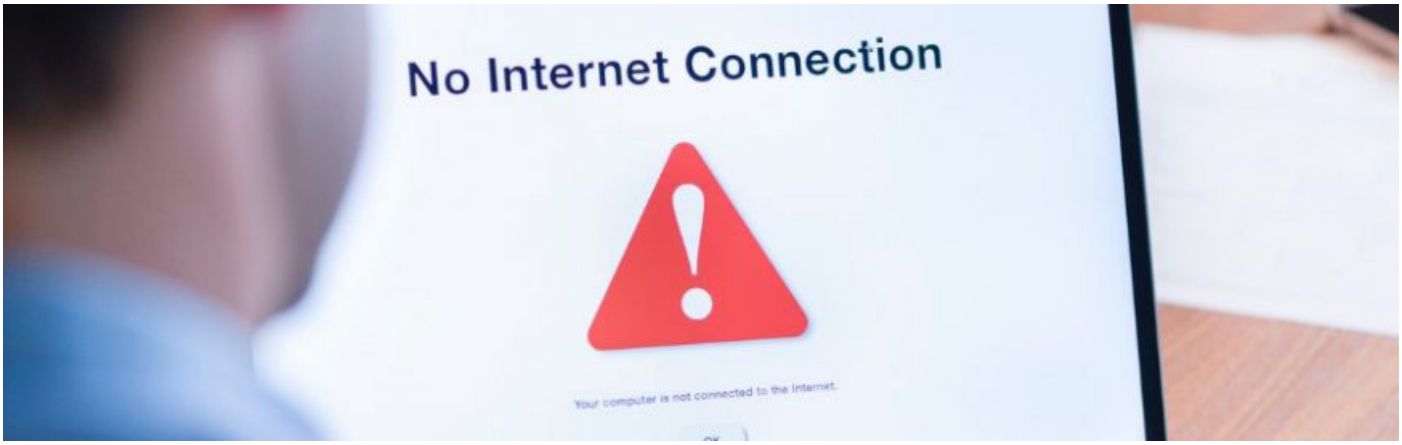
Find out more about the most common mistakes people make when creating passwords, cyber risks, and password best practices here:
https://lnkd.in/gRsZZsnw

#cybersecurity #passwords #security



Why Password Length Matters

Internet bandwidth requirements for remote workers



Working from home is here to stay, and more businesses will continue to implement either a fully remote work policy or adopt a hybrid work model strategy. Some employees, however, may find it difficult to be as productive at home as they are at the office, especially if they don't have sufficient internet bandwidth. But how much internet bandwidth is necessary to be able to work smoothly?

What is bandwidth?
Bandwidth refers to the maximum data transfer rate possible in a network or internet connection. It indicates the amount of data that can be sent over a connection in a given amount of time, and is usually expressed in bits per second (bps).

Imagine two computers with the same internet speed at 100 megabits per second (Mbps): the first computer only has a 50 Mbps bandwidth, while the second one has 100 Mbps. If they were to download the same packet with 500 megabits (Mb), the first computer would be able to do it in 10 seconds, while the second one could do it in just 5.

This is because the first computer's bandwidth is capped at 50 Mbps — even with a high-speed internet service, the limit of transfer would still be low. Therefore, the higher the bandwidth, the more data can be sent over a connection, contributing to faster uploads and downloads and a better internet experience overall.

How much bandwidth do you need for remote working?
To answer this question, you need to factor in the type of work that you do and the apps that you use. If your job mostly consists of sending emails, editing and writing on Google Docs, and communicating on Slack, then you can do your job with ease even with a low bandwidth. On the other hand, if your day-to-day tasks consist of frequently attending meetings through video calls, then you'd need a plan with higher bandwidth.

Once you have a clear picture of how much data you send and receive on an average workday, you can start looking for plans that can support your needs. And while you don't need to conduct virtual meetings in 4K quality, you also won't want your clients and colleagues to appear pixelated during a meeting. Neither would you want a session that gets choppy or cut off mid-conversation.

Here are the minimum requirements for the most common video chat apps used by remote workers today:

Zoom
For 1:1 video calling:

- 600 Kbps (up/down) for high-quality video
- 1.2 Mbps (up/down) for 720p HD video
- Receiving 1080p HD video requires at least 1.8 Mbps (downspeed)
- Sending 1080p HD video requires at least 1.8 Mbps (upspeed)

For group video calling:

- 800 Kbps/1.0 Mbps (up/down) for high-quality video
- For 720p HD video: 1.5 Mbps (up/down)
- Receiving 1080p HD video requires at least 2.5 Mbps (downspeed)
- Sending 1080p HD video requires at least 3.0 Mbps (upspeed)

Google Meet
HD video quality:

- Outbound signals must always meet a 3.2 Mbps minimum bandwidth requirement.
- Minimum inbound signals: 2.6 Mbps with two participants; 3.2 Mbps with five participants; and 4.0 Mbps with 10 participants

Standard definition (SD) video quality:

- Outbound signals must always meet a 1 Mbps minimum bandwidth requirement.
- Minimum inbound signals: 1 Mbps with two participants; 1.5 Mbps with five participants; and 2 Mbps with 10 participants

Skype
Video calling:

- HD: 1.2 Mbps (up/down)
- SD: 400 Kbps (up/down)
- The more participants, the higher the bandwidth requirement for downloads: 512 Kbps for three participants; 2 Mbps for five participants; and 4 Mbps for seven people. Upload requirements remain constant at 128 Kbps.

Microsoft Teams
Teams requires the same upload and download internet bandwidth for the following scenarios:

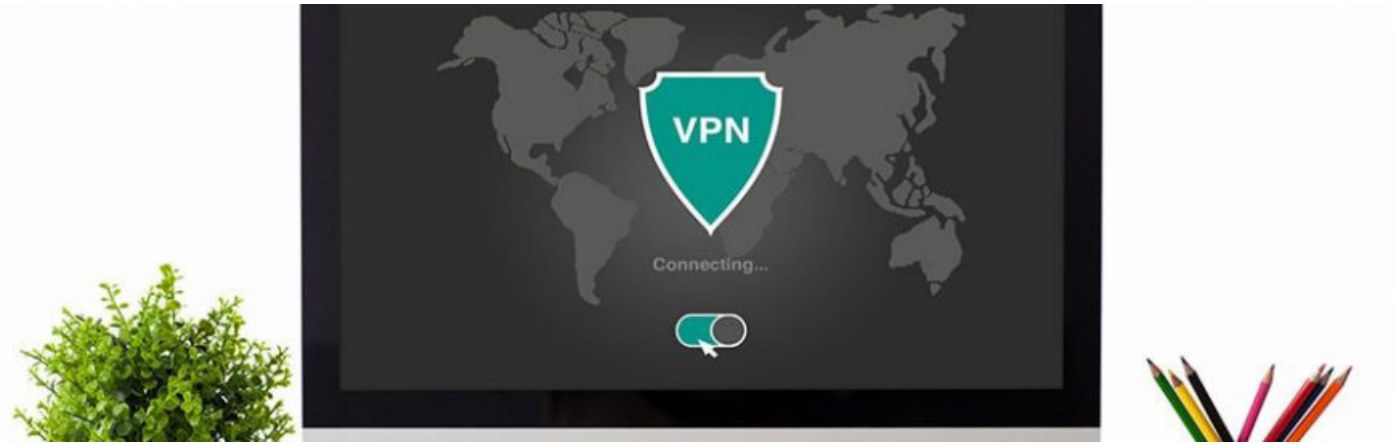
- At least 30 Kbps for peer-to-peer audio calling
- At least 1.2 Mbps for peer-to-peer HD-quality video calling at 720p
- At least 1.5 Mbps for peer-to-peer HD-quality video calling at 1080p
- At least 500 Kbps/1 Mbps for group video calling

If you're worried about your internet bandwidth, you can opt for audio calls instead of video calls. This considerably helps lower the information you need to upload and download.

For more tips and solutions on how you can work from home without a hitch, call us. We'd be happy to help.

Published with permission from TechAdvisory.org.

Surf securely with a VPN



There was a time when installing an antivirus program was enough to secure your data, but that's no longer the case today. Whether you want to keep your online activities hidden from third parties or prevent your data from being intercepted by hackers, you need to invest in a virtual private network (VPN).

What is a VPN?
A VPN creates a secure tunnel between your device and the websites you visit, protecting you from hackers looking to intercept your data. All data transmitted and received through this secure connection is encrypted, preventing any third party from monitoring your online activities.

VPNs can also disguise your location. Once you've established a connection to a VPN server, your computer acts as if it's using the same local connection as the VPN. As far as websites are concerned, you are browsing from the server's geographical area and not your actual location.

Why should you have a VPN?
VPNs augment your cybersecurity and help protect your privacy. For instance, it's generally considered bad practice to connect to public Wi-Fi networks, like those in cafes, libraries, and airports. This is because all data transmitted through these networks are unencrypted and, thus, are susceptible to exposure and theft. If you must use public Wi-Fi, make sure to activate your VPN. The VPN encrypts your data and keeps your connection secure as you surf the internet.

VPNs' ability to mask your location also makes them ideal for accessing geo-restricted websites and content. If you're traveling abroad and you find that critical documents or US websites are geo-blocked in your current location, just connect to a VPN server in the United States to regain access.

How do you choose a VPN?
Given the increasing demand for greater online privacy, VPNs are surging in popularity. When selecting which VPN to purchase, take the following into account:

Cost
There are free VPNs out there, but they likely keep logs of your internet activity or are filled with disruptive ads. That's why it's best to invest in paid VPNs like NordVPN and ExpressVPN. These paid options come with robust features, such as a large list of available servers, and configurations that bolster your data's security.

Location
Where your VPN's servers are located matters for several reasons. For one, the farther away the server you're connected to is, the greater the likelihood that you'll suffer latency issues. For a smooth surfing experience, it's best to connect to the closest available server. Additionally, if you want to avoid geo-restrictions, you'd want to connect to servers in the same location as the content you're looking to access. This means if you want to access research published in the United Kingdom, make sure your VPN has servers located in that country.

Capacity
Inquire with the provider or read their terms of service to determine how much data you're allowed to use. If your tasks require a lot of online resources, then you should choose a VPN with a high data allocation. Also, find out how many of the VPN servers are online; a greater number of online servers means the VPN is capable of supporting resource-intensive tasks

Device compatibility
Choose a VPN that can be used across multiple devices. If you use your laptop, tablet, or smartphone to do your tasks, then you should invest in a VPN that's compatible with all of these.

IP leak
Some VPN tunnels are not as secure as others. In some cases, the VPN could leak your IP address, enabling third parties to track your data and activities. Before buying a VPN, sign up for a free trial of the service if available. Activate the VPN and visit IP Leak. If the website says your IP address is being leaked, choose a different VPN.

If you need help in selecting the right VPN for your business, consult with our security experts today. We also offer comprehensive cybersecurity services so no hacker or third party can get their hands on your data.

Published with permission from TechAdvisory.org.

Velocity Technology is the right choice as your technology partner as we cover all areas from secure computer network design through to implementation and managed support.

As new technologies are established Velocity Technology will be able to design IT systems that will enable you to leverage technology to make your business perform better and enhance the usage of technology for all of your staff, wherever they are located.

Contact us today to find out how we can help your company to be more secure and effective.

Based in Asia and Providing IT Infrastructure and Cybersecurity Services Worldwide

Velocity Technology Limited

7th Floor Golden Star Building
20-24 Lockhart Road
Wan Chai, Hong Kong

Phone: +852 2915 5096
Fax: +852 2834 8852

Velocity Solutions Inc.

20/F, AXA Life Building
Senator Gil Puyat Avenue
(corner Tindalo Street)
Makati City, Philippines

Phone: +63 (2) 887 5344

sales@velocity-technology.com

www.velocity-technology.com