THE DOWNLOAD

GLASSEN TECHNOLOGY SERVICES

2020-2 〉 In This Edition:

From the Desk of Curtis Glassen

The IT industry has experienced many dramatic shifts and debacles during this year of crisis.

Manufacturers have struggled to keep up with the increased demand for items such as headsets, laptops, and webcams. To help our clients, we have begun stocking more of this equipment than ever before to help smooth out the ebbs and flows of availability.

Many businesses have been forced to adopt a remote working model. This shift has caused an increase in risks of data-loss and security threats.

We're doubling down on security and are in the process of rolling out laptop drive encryption, Multi Factor Authentication, and Phishing Email protection that uses AI to help protect against email-based threats for our MMS customers. These are big projects, but necessary to keep our customers IT systems and data secure in this crazy world we're in.

In this crisis together! -

~Curtis Glassen

SECURITY SPOTLIGHT:

Two Factor Authentication for Office 365: What, Why & How

Chances are high you've seen a message from an account you hold asking if you'd like to enable two-factor authentication (2FA). It might have seemed like the account provider was trying to make your life more complicated! However, they were actually using 2FA to deliver an extra level of security and protection for your credentials and the information you were accessing. Let's take a closer look at exactly what 2FA is, why it's important, and how it works.

What is 2FA?

Two-factor authentication is a security protocol that requires two different forms of identification to verify you are who you say you are before allowing access to an account. For example, in addition to entering your User ID and password (one form of identification), you might also be required to submit a verification code sent to your phone. This is just one method of 2FA, but there are many. Continued on next page..

Why is 2FA Important?

Simply put, two-factor authentication makes it harder for outside attackers to access sensitive or private information such as bank accounts or customer data. An Office 365 account that provides access to email, documents, financial statements, customer data, and a multitude of other information is exactly the kind of account that's most valuable to attackers. Think about a time where you've had to request a password change for your bank account – where does your bank send the reset link? To your email account! If hackers have access to your email account, they're able to see everything you see, putting your sensitive data at risk.

In addition, as phishing threats continue to rise, so does the risk of your user ID and password falling into the wrong hands. However, if 2FA is enabled, your User ID and password aren't enough to allow the attacker into your account, and your information will be better protected.

How does 2FA work?

2FA can be enabled through a variety of methods and will depend on how you choose to set it up. For Microsoft 365, you can choose to verify with a unique code sent to your phone, a phone call or by using the Microsoft Authenticator app. Once you set up your method and identify your computer and other devices as "trusted," you will only be prompted to enter a new security code any time you log in to a device that isn't trusted. That means you won't have to authenticate over and over again on devices you use regularly.

We also recommend setting up an additional verification method for Office 365 in case of a lost or stolen phone or mobile device. This enables a user to make use of the "sign in another way" link to access the account. If an alternative verification method has not been set, the user will need to work with the help desk to access and update the account.

Protecting business assets and customer data should be a top priority for any company and enabling two-factor authentication for Office 365 is a simple first step to getting it done. Contact us today to get started.

SERVICE INFO:

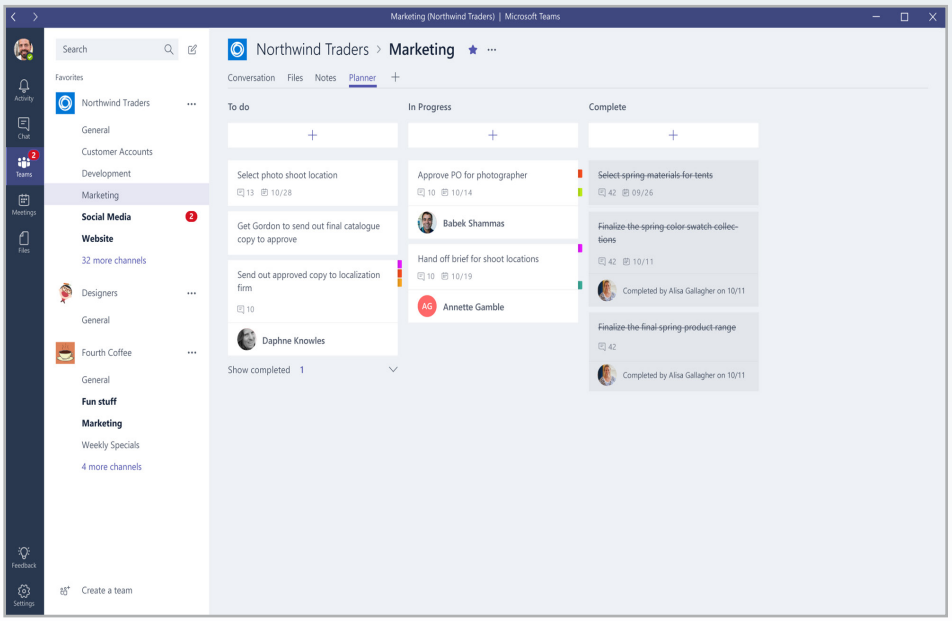
Microsoft Teams – More than just chat and calls

In part because of COVID and the need to communicate differently, Microsoft Teams has become extremely popular. The cloud service is included in most Office 365 plans and has a myriad of uses and features that go above and beyond workplace chat and audio/video calls.

"Teams" can be created within the software which can be used for:

- Filesharing
- OneNote Notebook Sharing
- Knowledge bases
- Group Chat
- Project Planners or To-Do Lists.

Teams users can also be used present and share your screen to guests outside the company. Dial-in (phone) conferencing can be added for only $4/user/month making it a much cheaper alternative to other legacy web conferencing solutions out there.



CUSTOMER SPOTLIGHT:

Midwest Assembly Warehouse & Distribution: West Bend, WI

With over 200,000 sq ft of warehousing and assembly space, Midwest Assembly Warehouse & Distribution needed an easy and cost-effective way to communicate with its staff out on the floor.

We provided a cloud hosted 3CX phone system and several inexpensive / refurbished iPhones with rugged protective cases. Using their existing Wi-Fi system, the iPhones use the 3CX app to make and receive calls – no expensive cell phone service required!

HELPDESK TECH TIP:

Shutdown Has New Meaning

Many users don't realize that Windows 10 has a feature called "Fast Startup" which is usually enabled by default. Fast Startup was developed to deliver a faster boot time when starting up your PC. While this sounds like a great idea (because let's face it, who wants to spend time waiting for their computer to boot up in the morning?), it can also cause performance issues.

To start, let's spend a moment understanding how Fast Startup works. When shutting down for the day, Fast Startup closes all open applications and users are logged out. However, in this state, Windows itself is never actually completely closed or shutdown. Instead, Windows is put into a "saved state." When you power the computer back up, Windows is simply resumed allowing you to access your computer more quickly, saving you time.

Since Windows is never actually restarted when Fast Startup is enabled, there are some issues that can occur as a result of using this time-saving feature:

System updates may fail to install

Typically, system updates happen overnight when computers aren't in use, and require a complete restart to fully take effect. If Fast Startup is enabled, your computer will shut down into its "saved state" and will not complete the update. You will need to manually perform a restart so system updates can finish installation and take effect on your computer.

Software updates may fail to install

Just like system updates, many software updates require a restart to complete installation. If you're taking advantage of Fast Startup, ensure that you restart your computer after installing or updating software.

System performance can degrade over time

As you use your computer – opening and closing applications, saving and deleting documents, etc. – it creates temporary files as it's working. After doing this for a while without a complete shutdown, you might notice your computer's performance slow down or start to get "buggy." Restarting will allow the computer to clear its memory and start fresh, often solving these issues.

So, while Fast Startup may provide some time-saving benefits, it can also cause some undesirable side effects. Because of this, we recommend you restart your computer at least once a week!

SERVICE INFO:

Coming Soon - A.I. Based Email Phishing Protection

We'll be begin slowly rolling out our Email Phishing protection system. Using Artificial Intelligence or "A.I." the system will be able to detect suspicious emails and display warnings at the top of your emails, making you aware of conditions such as:

• Never received email from this person before

• Other people in your company have flagged this message as suspicious

• The sender may look familiar to you, but the senders address does not match previous emails

• Senders domain is similar but different than previous messages

HELPDESK TECH TIP:

How to Safely Sanitize your PC, Laptop, or Mobile Device

Coronavirus has brought much attention to properly disinfecting surfaces, but keeping high-touch devices like your laptop, keyboard, and mouse clean and disinfected has always been a good idea. Here's a quick guide on how to get this done.

Do!

- Power down & unplug the device before cleaning
- Use a clean microfiber cloth lightly dampened with a 50/50 Solution of Distilled Water & Isopropyl Alcohol

Don't!

- Ever spray cleaning solution directly on the device, instead lightly spray solution onto a microfiber cloth. You should NEVER see liquid dripping from the device or cleaning cloth
- Use bleach or glass cleaner

Share Your Experience on Google

Google reviews help perspective clients gain insight before actively persuing a new business.

Do you have a quick moment to share your experience with Glassen technology Services?

If so - please visit Glassen.net/review

And to say *thank you*, we'll stop by your office with freshly-popped popcorn!

info@glassen.net 262-806-7286 GlassenTechnologyServices Glassen-Technology-Services