
When everything in your business is working as it should be, it's easy to believe that nothing will ever go wrong. However, seasoned business owners know that Murphy's Law often comes into play when things are otherwise running smoothly. Nowhere is this more obvious than with your IT environment.


If your server goes down, your phone system stops working, or your system gets hit with a virus, you're suddenly operating in crisis mode. Downtime affects your ability to serve your customers effectively and creates unplanned expenses. It frustrates your employees and damages productivity. And ultimately, IT problems can damage your professional reputation.

## How Managed Services Can Help Your Business

Working with a managed services provider (MSP) can help your business avoid some of the pitfalls of IT problems in the workplace. Managed services give a business the ability to focus on its core product and/or service offerings and operate more efficiently. The benefits are numerous, and include:

## 1. Proactive Monitoring

How great would it be to be able to stop a problem from happening in your infrastructure? Your MSP constantly monitors your systems for issues, often resolving them before they become a problem.



*Continued on next page*

*Continued*


## 2. Routine Maintenance

Hardware failure can create an all-hands-on-deck scenario as you scramble to repair malfunctioning equipment. Ongoing maintenance provided by your MSP, however, helps to keep your technology up-to-date and can actually extend the life of your hardware.

## 3. Instant Support

There will be times when you simply need help with your tech. Managed services typically include a support component, which allows you and your staff to simply call or email when you need assistance. Often, your MSP can resolve problems remotely and limit inconvenience to you and your staff.

## 4. Built-in Repairs

Your bottom line can take a hit when it comes to repair fees, particularly if it takes more than one repair service to fix a single issue. Managed services perform repairs quickly and economically in accordance with your agreement.

## 5. Consistent Monthly Rate

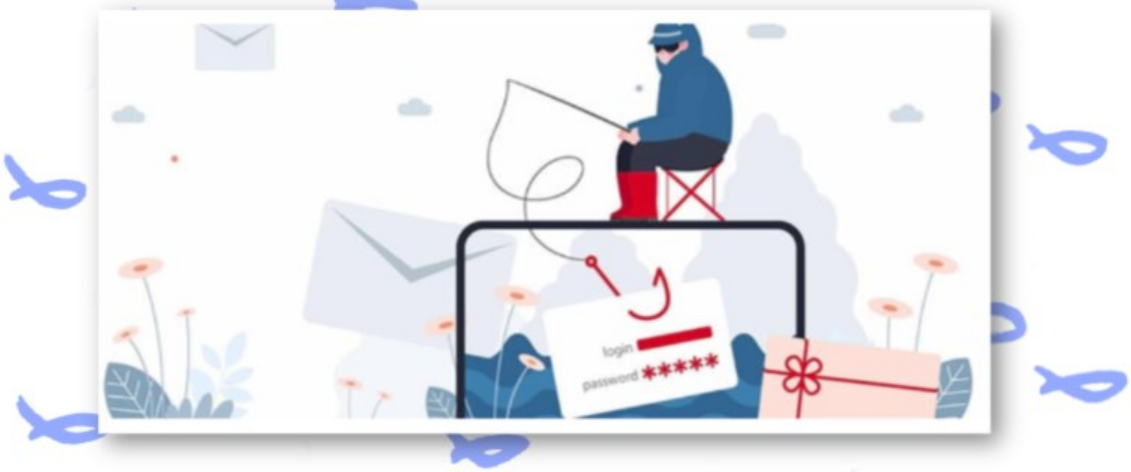
IT budgets can be unpredictable without a managed services agreement. For a flat, monthly rate, however, you can better control the peaks and valleys that often accompany IT expenses.

## Get a Handle on Your IT With Managed Services

For the small and midsize business, managed services can provide many of the same advantages that an in-house IT department brings to large corporations. Limit your downtime and reduce the hassle of IT problems, all for the cost of a regular monthly fee. Reduce the frustration that can sometimes accompany technology and improve staff productivity and workplace culture. Managed services provides a single source for maintaining a robust IT environment, a clear advantage over trying to fix issues as they arise.

Pittsburgh Computer Solutions can help your business to determine the right mix of managed services offerings for your business' unique needs. Contact PCS at 724-942-1337 for more information.

# An Employee Received a Phishing Email - Now What!?




One of the reasons why phishing attacks are so successful is that they're always evolving. There is always a new kind of phishing e-mail going around every day.

Dealing with the repercussions of a phishing attack is not only time consuming but costly. One careless click has the potential to compromise your entire network, so it is important that everyone works as a team to protect the company. Make sure there is a system in place to report attacks, and make sure all of your employees understand how important it is to follow through in reporting it. Deleting the offending email is not the solution—IT needs to know that your company is being targeted. Train your employees to contact your IT department immediately so that IT can take appropriate actions, and create a feedback loop to help improve the email filter.

While structured annual or semi-annual training is recommended, employees should also receive on-the-fly training when an attack occurs. If an employee clicks on a phishing link, they should receive immediate feedback and additional training. Review the email with them, show them the red flags and indicators they missed, and provide additional training materials to help them avoid being phished in the future.

PCS announces its partnership with Vade Secure for Office 365. Vade Secure's email security solutions help protect users from advanced cyberthreats, such as phishing, spear phishing, and malware. Vade Secure users receive a warning banner at the time-of-click if a URL has been identified as phishing. If the user clicks on a phishing link, IT receives a notification, along with a link to a phishing training handout. This ensures they are immediately aware of their mistake and connects the incident with the training. If spear phishing is suspected, the user receives a warning banner in the email, advising them to proceed with caution.


Vade Secure is the global leader on anti-phishing, spear phishing, malware and ransomware filtering. Fed by data from more than 600 million mailboxes, a predictive email defense solution leveraging AI (Artificial Intelligence) and machine learning to protect users from unknown targeted attacks. Vade Secure also features behavior-based anti-malware, insider attack protection, anti-phishing, anti-spear phishing, and protects against CEO fraud.

This product leverages Office 365's built-in capabilities for encryption and backups. Vade Secure for Office is the only native email security solution that sits inside Office 365.

MX (Mail Exchanger) records are complex for end users and difficult to add and filter this type of solution. For those reasons, Vade has no MX redirection, and instead filters internal email flow to remove quarantined emails from the inside with no training necessary thanks to their native Office 365 interface.

Activation could not be easier. All user must do is provide Vade Secure with a tenant ID, get logged in using Office 365 credentials, and activate journaling. Vade will then begin populating. The dashboard displays threats detected, classification types for each threat detected, a graph for trend visibility, and information surrounding the last targeted attacks with data and time, who they were from, who they were sent to, what the subject was, and the classification.

From what we saw of the administrator interface, it is customizable, featuring compliance management with auditing, retention policies, tags, journal rules, etc. The journals are used to record all communication in support of an organization's email retention or archival strategy.


The user interface uses the junk email folder to dump spam and phishing emails instead of a quarantine method. The dashboard shows recommended actions, customizable folders Vade Secure automatically deposits messages into according to type and categorizes spam. It will check every time a user clicks an email and redirect them to Vade Secure to detect any spam or phishing attempts.

**When in doubt, check it out.** Vade Secure allows you to check a URL or site to see if it contains any phishing activity: http://isitphishing.ai/index.php. It also has a live feed you can watch and see what sites they pick up on that contain phishing attacks. Pretty cool!

Vade Secure's intuitive solution is fully transparent to users, and is thoroughly customizable for administrators. With email encryption, spam filtering, and virus/malware protections, it is worthy for anyone looking to protect on-premises email or cloud email, guard against email fraud protection and obtain added assurance with email backup.

Vade Secure has developed a full set of security features against the most sophisticated email scams.

Call PCS today and schedule to see a demo for Vade Secure's email security solution.
724-942-1337


# Graymail

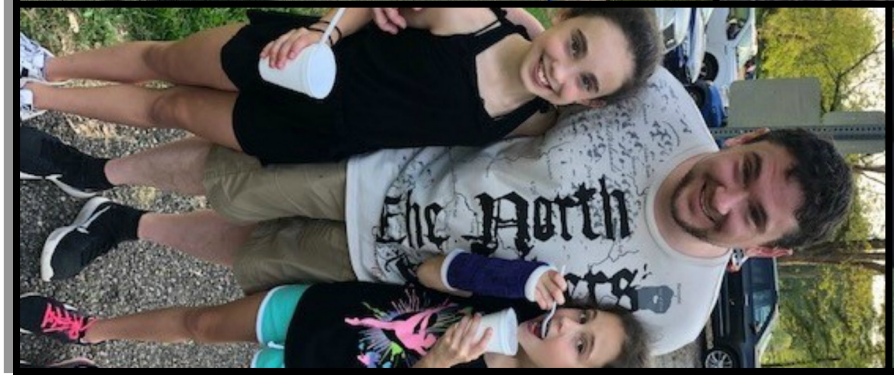
Graymail is a word used to describe "unwanted" email from a company or website. At some point a user would have agreed to receive the email via subscription list opt-in, but now considers the messages to be unwanted.

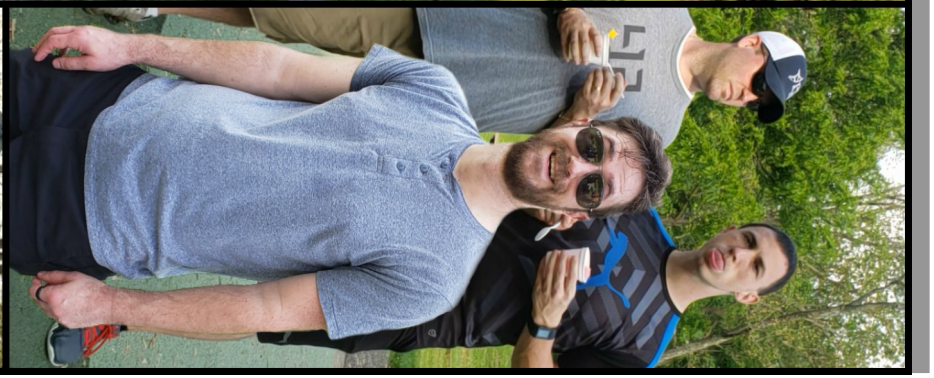
The word "gray" is used because the email falls between the "black and white" area of email spam and legitimate welcome email. Some recipients might consider this type of email spam (unwanted email) while others find the email useful (wanted email).

Examples of graymail include newsletters that you sign-up for (and often forget about but receive for years), messages you receive when you sign up for an online service or the automatic notifications received from online services, including social networking sites.

# Fun Times with the PCS Family





ESCAPE ROOM
PITTSBURGH

# TOMB EXPLORER

THE END.