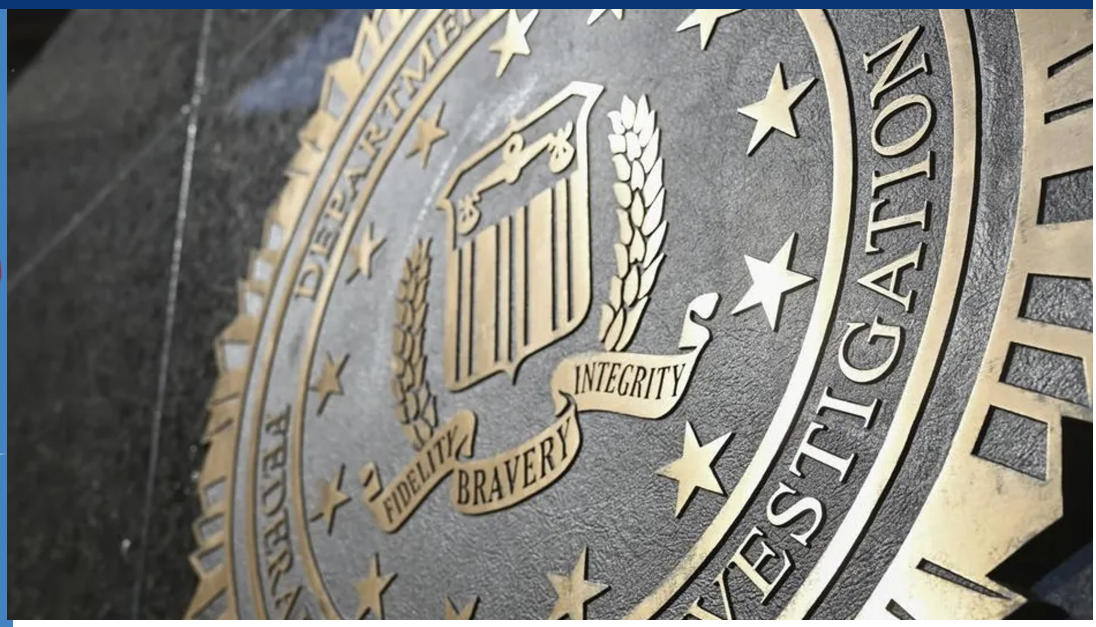
DTS DanTech Services
Computers under control!™

Technology Times February 2025 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:



FBI Warns Gmail, Apple Mail, Outlook Users—Emailing These 2 Words Is Dangerous

Zak Doffman

The cyber threat landscape is getting worse. Driven by new and frightening AI-fueled threats, it is becoming ever harder to tell real from fake, safe from sorry. With "criminals exploiting generative artificial intelligence (AI) to commit fraud on a larger scale, which increases the believability of their schemes," as the FBI warned last month, it would be great to know some of the telltale signs to help us root out the threats now sneaking into our inboxes.

The vast majority of cyber attacks start with a phishing email, and so better security of our Gmail, Outlook and Apple Mail inboxes, as well as any others, would make a huge difference. Email remains a backward technology in need of a refresh — it is clear the platforms can do a better job keeping us safe, and to make better use of AI to filter out threats.

Sometimes, though, it's the little things that help. So it is with the latest FBI warning, which gives you one strong indicator that an email needs to be deleted before it's read or even opened. "Pressure to 'act fast'," the bureau says could easily be "a sign of a scam." I will go further. Any email that stresses urgency or the need to "act fast" — unless it's from someone you undeniably know and absolutely trust — should be avoided. Those two words are dangerous.

Microsoft echoes this, warning that you should "be suspicious of emails that claim you must click, call, or open an attachment immediately. Often, they'll claim you have to act now to claim a reward or avoid a penalty. Creating a false sense of urgency is a common trick of phishing attacks and scams. They do that so that you won't think about it too much."

- Continued on page 3

Hackers Exploit Microsoft's AI to Create Harmful Images

Cybercriminals used stolen login credentials to access Microsoft's Azure OpenAI service and bypass safeguards for the DALL-E image generator, which they used to create "offensive and harmful" images.

After they used these resources, the hackers resold access to other malicious actors, providing them clear instructions on ways to use the tools\ to create illicit content. They used custom software called "de3u" to prevent Azure OpenAI from filtering harmful content.

Although it's not clear what kind of offensive imagery was generated, it is known that the de3u tool could stop OpenAI from changing text prompts that contained certain keywords to trigger content filtering.

Microsoft seized the domain "atism.net" used by the hackers and revoked their access.

After the seizure, Microsoft observed the hackers taking steps to hide their activities, including deleting specific pages on Rentry.org, the GitHub repository for the de3u tool.

Microsoft has implemented new countermeasures and safeguards to prevent further misuse.

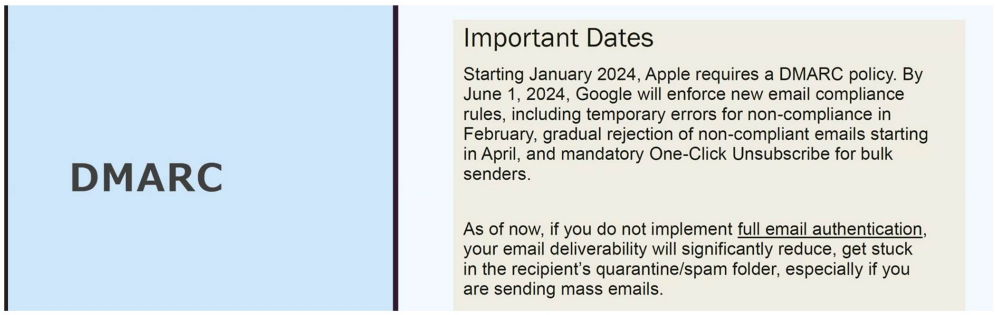
The hackers discussed the crackdown on forums like 4chan, indicating they might target other AI image generators in the future.

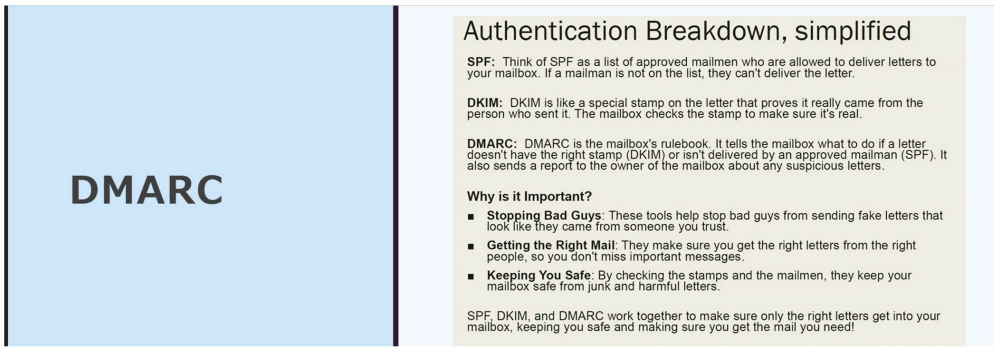
The importance of DMARC and email delivery

My junk mail list is filled daily with emails that, in many cases, should be delivered to my inbox. For the very good reason of attempting to limit spam or junk mail, numerous changes have been made over the last few years to tighten delivery requirements.

There are three primary records that are critical to email delivery: SPF, DKIM, and DMARC. When all three requirements are met, email delivery rates from compliant services go up and spammers, scammers, and slammer emails go down. Adoption of DMARC has become a requirement—or will be soon. All of the major services are making use of these new requirements.

This article is about DMARC requirements:

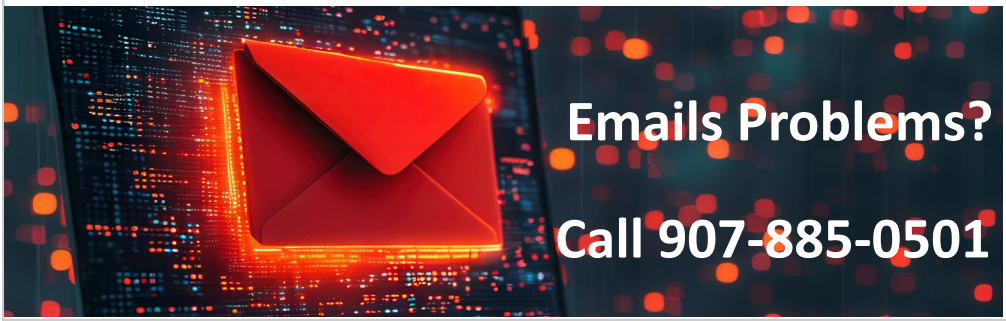




Does your domain deliver DMARC verification? Go to: Network Tools: DNS,IP,Email, insert your email domain (what's after the @ sign), and select DMARC from the dropdown menu to the right. Other records can also be checked here. Check the SPF record for your domain. Do all of the email sources for your email domain show in the SPF record?

Check your DKIM record (although this one is a bit tricky). It requires additional information. If your email is delivered by Microsoft Exchange services, you'll need to add ":selector1" after the domain name—or any other DKIM identifier, or you're receive an error.

Do your results return GREEN? You should be good to go (as long as all the requirements are in place). Do the results show RED? There's work to be done. DanTech Services provides services that provide solutions to the above problems—and more! Too many SPF record lookups are a problem. We have a solution. Let us know if we can help!



FTC Issues Final Warning to GoDaddy Over Security Failures

The Federal Trade Commission (FTC) has been warning GoDaddy to address a number of security concerns from as far back as 2018, but the web hosting giant has yet to resolve these issues.

In January, the FTC issued a final warning to the company about its security protections, accusing GoDaddy of misleading millions of web-hosting customers and failing to protect its hosting services sufficiently. The complaint lists at least eight cybersecurity violations, including failure to implement standard security tools and practices and failure to log security-related events.

These data security failures led to several major security breaches between 2019 and 2022, and resulted in threat actors gaining access to customers' websites and personal information.

"The FTC is acting today to ensure that companies like GoDaddy bolster their security systems to protect consumers around the globe," said a spokesman for the FTC's Bureau of Consumer Protection.

Talk to us about your web-hosting problems!

"Emailing These 2 Words Is Dangerous" - continued from page 1

And Google says exactly the same: "Slow it down. Scams are often designed to create a sense of urgency, and often use terms like 'urgent, immediate, deactivate, unauthorized, etc.' Take time to ask questions and think it through."

This latest FBI warning comes as part of a package of suggested measures to protect against scammers using major disasters as a lure to trick victims — the California fires by way of example. And that's the other warning sign.

Criminals need a hook, and what better hook than a disaster that may have impacted you directly or where you might want to offer charitable assistance. Or it could be very different, recovering a TikTok account during the shutdown, for example.

ESET's Jake Moore warns that "forcing people to act quickly and think later can be an effective way to make people respond immediately without leaving any time to err on the side of caution. Therefore, however persuaded you may feel to respond, it is always worth remembering to take your time and carry out due diligence where necessary."

And CISA — the U.S. cyber defense agency — suggests being very wary of any emails that use "urgent or emotionally appealing language, especially messages that claim dire consequences for not responding immediately... If a message looks suspicious, it's probably phishing... However, if you think it could be real, don't click on any link or call any number in the message.

Look up another way to contact the company or person directly." That said, more sophisticated phishing emails are looking much less suspicious than they ever have before. AI helps tone language and removes mistakes in spelling and grammar, it also crafts realistic imagery and can mimic any brand.

The FBI's phishing advice remains as valid as ever — notwithstanding that AI makes it more difficult to identify a threat with a cursory scan of the copy and imagery:

- "Remember that companies generally don't contact you to ask for your username or password.
- Don't click on anything in an unsolicited email or text message. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.

Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions."

"Impressive manipulation tactics are constantly improving," ESET's Moore told me, "and can often leave people stunned at how easily they were influenced.

Scam communication draws on heavy emotional influential messaging and manipulating tactics which can work very efficiently on unbeknown victims." You have been warned — do not "act fast" after all.

KingSmith Fitness' Walking Pad Treadmill

Discover the WalkingPad P1 folding treadmill. A classic model that offers exceptional quality and performance. Perfect for home use, easily folds for storage. Loved by thousands for its streamlined design. No more excuses – it's time to invest in your fitness and well -being. Whether adding a walk to your workday or exercising while watching your favorite show, the P1 is perfect. When you're done, it folds to the size of a small suitcase and can be easily stored under a bed or couch. Stay fit and active with the WalkingPad P1.

Unique Foldable Design: We invented the folding treadmill known as a WalkingPad to save you space and time.

FootSense Tech: Walk toward the front of the walking pad and it automatically speeds up, carefully slow down as you move to the back and it slows down nearly mirroring your pace.

Comfy Cardio: We have built layers of shock-absorbing tech into the P1 to reduce the impact on your body.

Remote Data Display: Your steps, calories, distance and time are shown right on the remote.

Professional Running Deck : Combining layers of patented tech makes it possible to remove some of the impact on your joints. Compared to running on a hard unforgiving road you will be happy you chose a WalkingPad. Plus, noise is reduced as well, your neighbors will thank you.

Cyber Threats Evolve with Increasing Complexity

Cybercrime is becoming a bigger threat every day, affecting everyone from regular consumers to entire governments. A 2022 Hiscox report found that 43% of companies experienced a cyberattack, with 20% of those being so severe they put the business at risk of shutting down. The financial impact is massive—by 2023, the average cost of a single data breach was projected to hit $5 million, with some estimates, like IBM's, reaching as high as $9.44 million. Not surprisingly, the demand for stronger defenses is skyrocketing. The $155 billion cybersecurity market is expected to more than double to $376 billion by 2029.

One scary trend in cybersecurity is the rise of deepfake technology. Hackers use AI to create incredibly realistic fake videos, images, and audio that are almost impossible to detect. A VMware survey revealed that 66% of IT leaders experienced deepfake-related attacks in the past year—an alarming jump from previous years. Deep-fakes make it easier for cyber-criminals to pull off scams like business email compromises (BEC) or bypass face-to-face verifications. The spread of 5G has made this threat even worse by ena-bling real-time manipulation of media.

To fight back, many companies are turning to AI-powered cybersecurity tools. These systems can detect threats faster than humans and even take action to stop them before they cause major damage, cutting the average cost of a breach by $2.22 million. With the ability to analyze millions of files in milliseconds, AI tools are helping businesses stay one step ahead. Still, cybersecurity remains a constant game of catch-up as attackers get more creative, which is why ongoing investment and innovation are so critical in this space.

Is You Business Data Safe?