This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

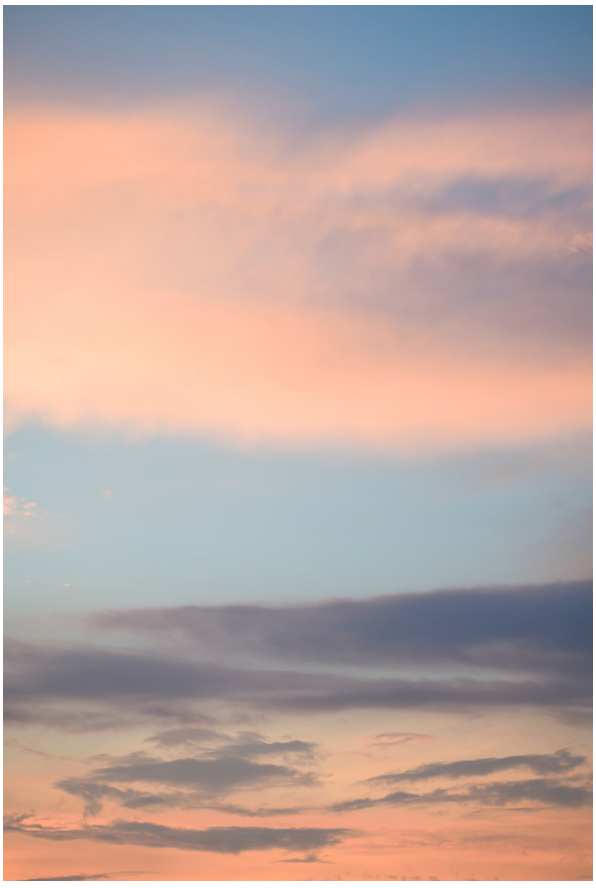
Becoming CYBERMINDFUL

For you. For everyone.

IN THIS ISSUE:

IS YOUR HEAD IN THE CLOUD?

Welcome! This time we're **Becoming Cybermindful** with some info about cloud computing. It's a term we see floating around a lot (no pun intended), but what does it really mean? "The cloud" is really just a lofty way of saying "a bunch of computers somewhere else." Let's talk conveniences and cautions.



Life in the Cyber Clouds

Think about services like Gmail. You check it at work, you check it at home, you check it from your phone ... and it's the same everywhere! Twenty years ago this would've been a minor miracle, but now we've come to expect this kind of consistency and ubiquitous access to tools and storage.

That's the cloud at work: with your email handled by the provider's mail servers (instead of your local computer), all you need to reach it is an internet connection. In fact, if you can access a service or piece of data regardless of the device you're using, it's typically in the cloud.

What's not in the cloud? Well, that Excel spreadsheet and the family pictures you saved to your desktop – you can't get to those unless you're at that particular computer. But if you save them to an online storage tool? Then they're in the cloud and you can get to them from any connected device.

Services such as Google Drive, iCloud, Amazon Cloud, Shutterfly, and Box are examples of cloud services and cloud storage – convenient, and often free of charge. It's all so

Weird email from someone you know? Check with them before clicking.

beautiful up there in the cloud-speckled sky. But alas, the weather isn't always sunny and not all clouds are the same.

Steering Clear of Storm Clouds

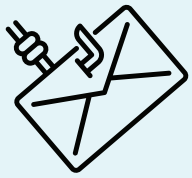
All our stuff, all the time, everywhere we go? We love the cloud! We should put *everything* in the cloud, right? Well, not so fast – once you trust your information to the cloud, it's no longer completely under your control and a few things could go wrong:

- Data breaches – someone you didn't authorize has accessed your information
- Data loss – your data has become irretrievable
- Denial of service – someone is keeping you from accessing your data

With these risks in mind, here are some things to consider in the technical troposphere:

Sharing settings.
Cloud services generally have settings that let you determine who else can access your information. Be deliberate about who gets access and whether you permit those folks to share access with even more people.

Life on the ground.
The more sensitive information is, the more you may want to keep it on terra firma (on a single computer backed-up on an encrypted, portable hard drive or in a specific location designated by your company). At a minimum, check with your organization's IT team before storing any data



Scam Self-Defense: Spear Phishing

In addition to generic, garden-variety phishing, you might someday encounter a very personalized, spoofed email. This is known as "spear phishing" because it singles out an individual by name and provides a degree of insider knowledge in its request. Where does this information come from? Organizational websites, our own social media postings ... a little bit of online research can expose just enough info to appear slightly credible.

If you receive an odd request from someone supposedly within your organization, look twice. There may be some suspicious inconsistencies:

- ✗ The reply-to email address might be an external account

protected by law (medical information, personal identifiers, financial data) in the cloud.

Encryption when uploading or downloading data from the cloud.
Make sure that your browser or app requires an encrypted connection before you upload or download your data. Look for the "https://" or the padlock beside the URL in your browser.

Your options for data protection and recovery.
If the cloud provider is hacked or loses your data, will this be remedied? Well, if it's a free service (as many online services are) you get what you pay for – so caveat emptor!

The key to your castle in the cloud.
Cloud services require a password to access your files, so make it a good one – longer is better. And if a service offers multi-factor authentication, use it.

Hope that cleared things up. You know, made things less foggy. (Sorry, couldn't resist!)

- ✗ The sender's signature block may be different than usual
- ✗ The request itself might be out of context and request immediate action

If so, don't reply. Forward the suspicious email to your IT support team for verification or reach out to the sender separately, apart from any contact info provided in the message.

And that's it for today. Until next time, stay Cybermindful ... even when your head's in the clouds!

Learn more about Becoming Cybermindful at go.udayton.edu/cybersecurity

THIS PUBLICATION IS PROVIDED BY:

University *of* Dayton
Center for Cybersecurity & Data Intelligence

OHIO CYBER RANGE INSTITUTE