Newsletter: April 2021

ON CLOUD NINE

A review of the latest security threats and how you can avoid them

THIS MONTH'S TOPICS:

The cloud may seem like a mysterious thing, but so much of what we do and how we do it operates through the cloud. Our job may involve using cloud services to store and access company data when we work remotely. Our personal files and information may also be saved to the cloud or use cloud services to make certain applications and tools accessible from anywhere.

It may be difficult and quite frankly scary to trust that our information is safe in these seemingly intangible locations, but these cloud service providers generally take their security protections very seriously. However, they are only responsible for ***their*** security; the rest is up to us. Take a step back and think about where your data is and if your protections are enough to keep a cybercriminal at bay.

Understanding the Cloud

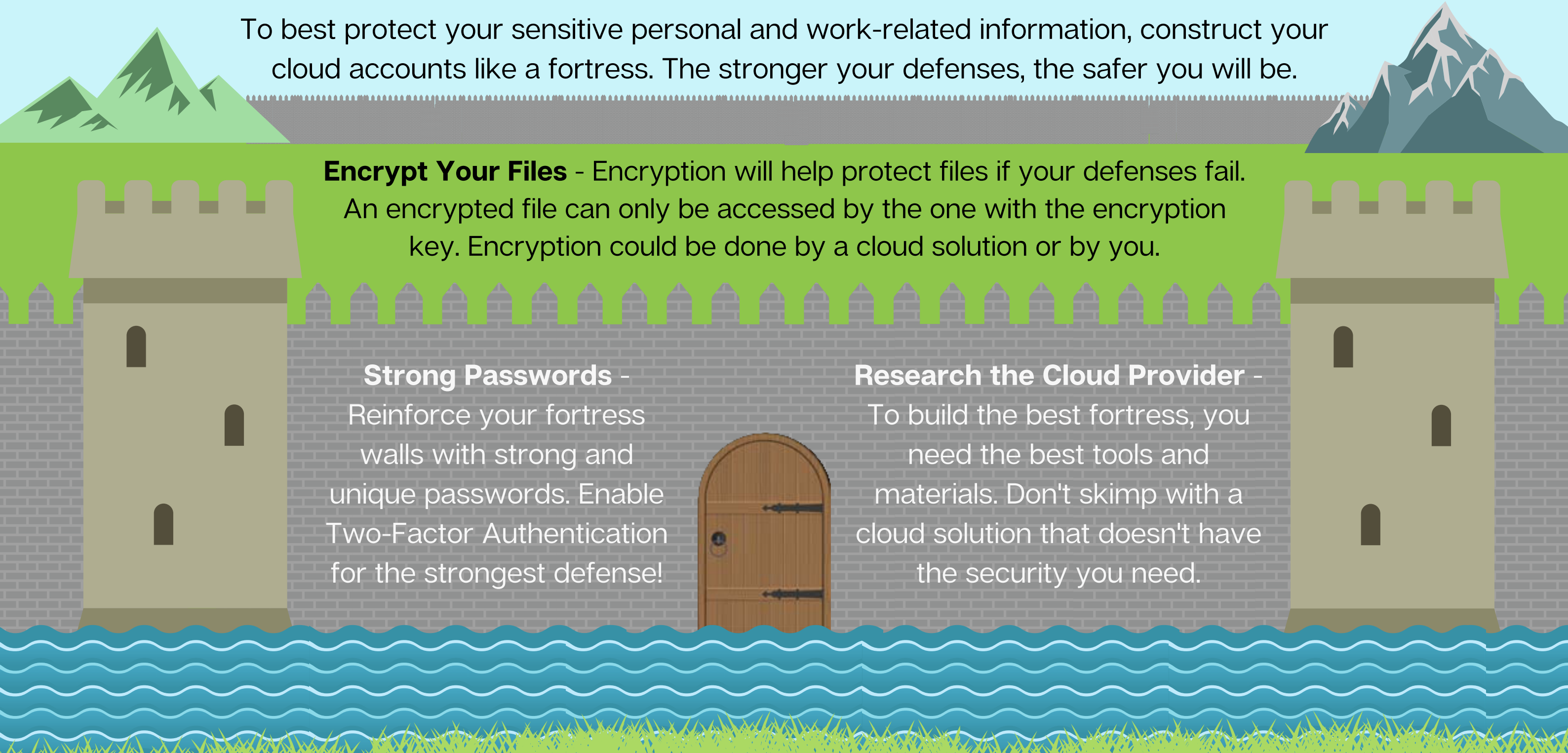
The cloud is how our digital information is stored so it can be accessed remotely from anywhere. Whether we know it or not, we access and use the cloud regularly. It could be a backup of our files, music, photos, or a social media or email service.

Although keeping data in the cloud should be relatively safe, there are risks if the proper security precautions are not met.

Cloud Jacking occurs when a cybercriminal takes over a cloud account. They may get access by guessing a weak or compromised password, or through a social engineering attack. Once exposed, the cybercriminal has access to a wealth of information, potentially leading to a breach, blackmail, or identity theft.

TIPS FOR STAYING SAFE IN THE CLOUD

To best protect your sensitive personal and work-related information, construct your cloud accounts like a fortress. The stronger your defenses, the safer you will be.



Encrypt Your Files - Encryption will help protect files if your defenses fail. An encrypted file can only be accessed by the one with the encryption key. Encryption could be done by a cloud solution or by you.

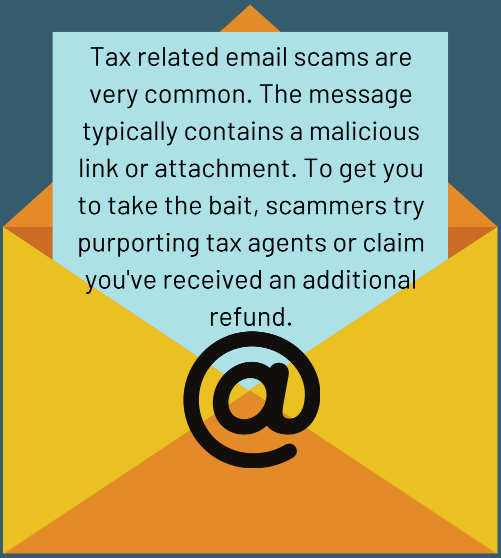
Strong Passwords - Reinforce your fortress walls with strong and unique passwords. Enable Two-Factor Authentication for the strongest defense!

Research the Cloud Provider - To build the best fortress, you need the best tools and materials. Don't skimp with a cloud solution that doesn't have the security you need.

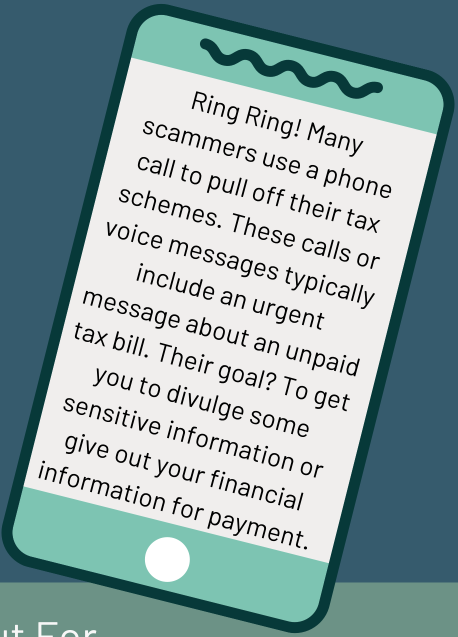
Sign out when not in use - Don't give a criminal an opportunity for cloud jacking by leaving your castle door open. Sign out of your account when finished, and avoid using a shared computer or letting your browser remember your cloud passwords.

TAX SCAMS

Preparing and submitting tax returns can be an overwhelming task. With so many deductions, exemptions, and credits to worry about, unfortunately, a tax scam is another pain point on that list to be cautious of.



Tax related email scams are very common. The message typically contains a malicious link or attachment. To get you to take the bait, scammers try purporting tax agents or claim you've received an additional refund.



Ring Ring! Many scammers use a phone call to pull off their tax schemes. These calls or voice messages typically include an urgent message about an unpaid tax bill. Their goal? To get you to divulge some sensitive information or give out your financial information for payment.

What to Watch Out For

Threats - Scammers often make threats to encourage action. This could be imprisonment, license revocation, or large fines. Real tax agents claim these types of threats would never be made via a phone call or email.

Impersonations - Scammers try impersonating a tax preparer, federal agent, or other entity with power. This social engineering method of Authority is a common tactic to grab the attention of their prey.

Work-Related Tax Scams - Many experienced scammers target team members in the Finance department. They generally spend more time gathering information on your company and job role to craft their attack. Before making payments or submitting information, verify with your supervisor.

Top Tips for Tax Time

Choose a reputable tool or personal filer to help with taxes. Find a trusted source to help you with your tax filings. Make sure the preparer or tool takes the security of your information seriously.

Backup important files securely. When submitting your taxes, it is helpful to retain a digital backup of your filing. Choose a secure solution and make sure you've got strong password security set up.

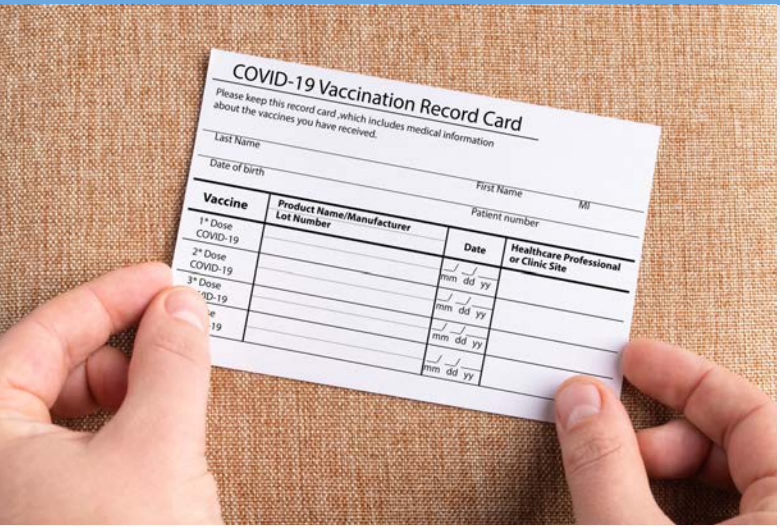
Always be on the lookout for tax scams. It's not just tax season, these scams happen all year round.

Report any potential scams to your supervisor and IT when they occur at work. If you've fallen victim outside of work, contact your local consumer protection agency.

SCAM OF THE MONTH

Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Marcie had been waiting patiently for her chance to get the COVID-19 vaccine. When her time finally came, and her first dose was administered, she wanted to share her excitement on social media. Marcie snapped a cute selfie holding up her vaccine card. The card didn't contain much information, just her name, date of birth, and the vaccine details. She posted the picture online and shared it publicly, not just with her friends. A week later Marcie received a call to book her second vaccine but the scheduler said they need her government identification number and more personal information to complete the booking. Marcie obliged, not realizing she just gave away her information to a scammer.



COVID-19 Vaccination Record Card

Please keep this record card, which includes medical information about the vaccines you have received.

Last Name First Name MI

Date of birth Patient number

Vaccine	Product Name/Manufacturer Lot Number	Date	Healthcare Professional or Clinic Site
1st Dose COVID-19		mm dd yy	
2nd Dose COVID-19		mm dd yy	
3rd Dose ...D-19		mm dd yy	
...e ...19		mm dd yy	

Did you spot the red flags?

- Marcie posted her picture publicly, allowing anyone to see it.
- Her picture contained valuable personal information which was used against her in a follow up scam.
- The scammer posed as a vaccine scheduler with knowledge from the simple image Marcie posted.

Social media sites are great for sharing information with friends and family but watch what you post and to whom. Keep any posts containing your personal information private, so only those in your circle can see.

Vaccination cards are wildly popular right now among the cybercrime community. Vaccination cards are being forged and sold through many online channels. The forged card could be used by others to receive your second dose or provide additional information for scammers to use in their attacks against you.

Although it may not seem like much, an image or post containing your personal details such as name and date of birth can be a goldmine for a cybercriminal. This information could be used for additional spear phishing attacks or identity theft.

HOT TIP If you want to post about your recent vaccine, you still can! Just keep the post private and avoid sharing any details from the vaccination card.

Every Dark Cloud Has a Silver Lining

Key Takeaways

With so much of our personal and work information saved in the cloud, it is critical we don't expose ourselves to cloud jacking. Don't let a poorly configured cloud rain upon your parade.

Treat your cloud accounts like a digital fortress. Choose trustworthy vendors and make sure your passwords are strong and unique. For advanced protection, enable two-factor authentication (2FA) and encrypt your files saved on the cloud.

Your vaccination card is important, don't let it slip into the wrong hands! Posting this type of personal information leaves you exposed to identity theft and additional scams involving your vaccine.

Remember that tax scams occur year-round. Watch for threats and impersonations over the phone or through email. If your job involves tax-related material, be especially cautious of targeted attacks and verify with your supervisor before completing an out-of-the-ordinary task.

Cybersecurity Cryptogram

A Cryptogram takes each letter of the alphabet and replaces it with a number. Using the key at the top, find the appropriate letters that correspond with the phrase below. We gave you a few to start, can you find the hidden phrase below in this month's puzzle?

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
				18									15		16										

_ P _ _ _   _ _ _ _ E _ _   _ _ _ N _
12 16 3 5 13   2 7 17 24 18 3 2   22 3 5 15 25

_ _ _   _ _ _ _ E _ _ !
23 12 4   1 13 17 24 18 3 2

Answer: April Showers Bring May Flowers!