NOVEMBER 2023 ISSUE NEWSLETTER

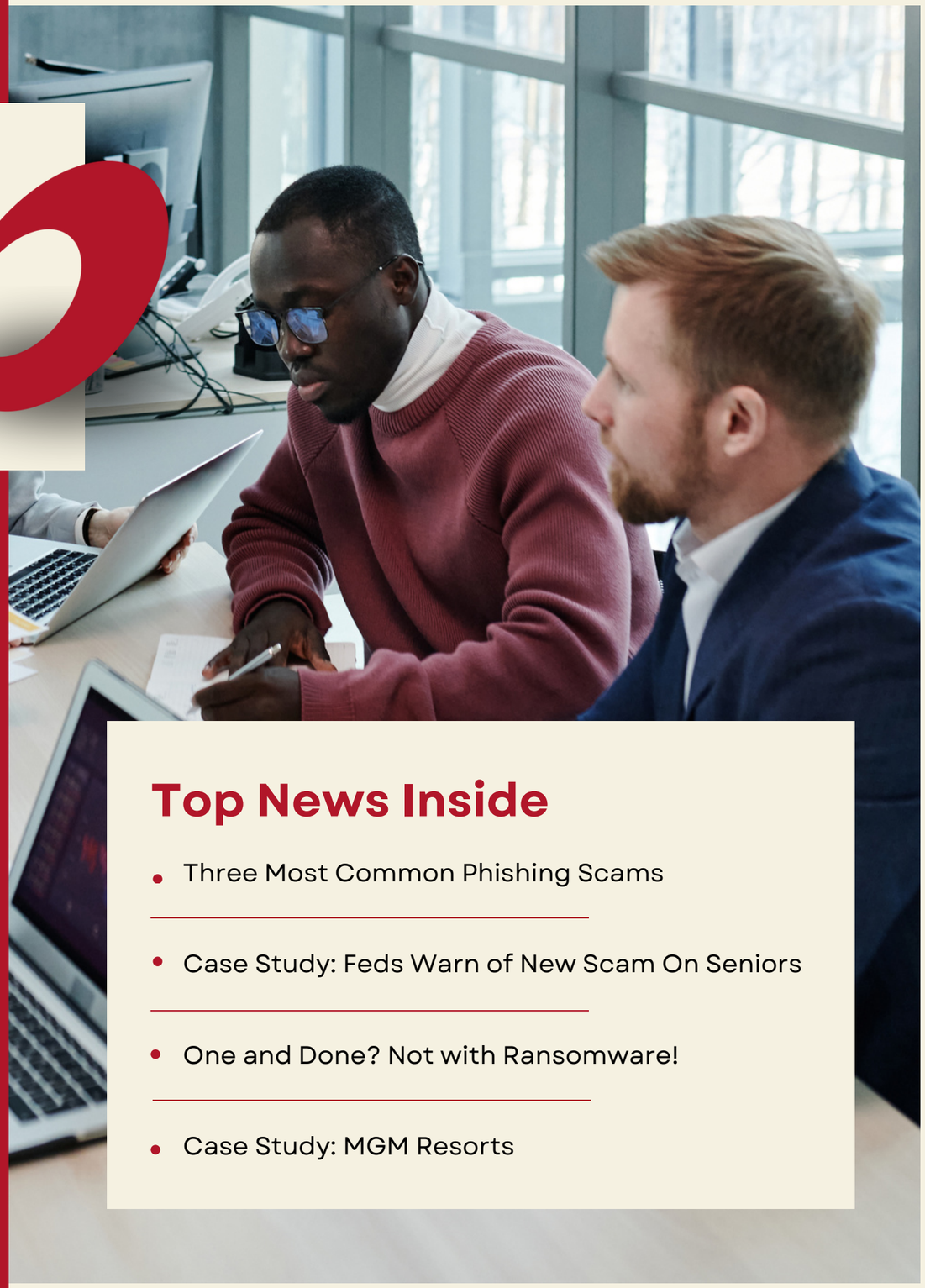
REMEMBER, REMEMBER, SECURITY IN NOVEMBER!

What should you do when you find corrupted backup files? Discover a virus? Get hit with ransomware? We have answers to ALL your tech questions!

3 Tech Tips You Should Know

- Keep your software up to date. Software updates often include security patches that can help to protect you from known vulnerabilities.
- Be careful about what links you click on and what attachments you open. Phishing emails and malicious attachments are a common way for attackers to gain access to your computer or online accounts.
- Use strong passwords and enable two-factor authentication (2FA) whenever possible. 2FA adds an extra layer of security to your accounts by requiring you to enter a code from your phone in addition to your password when logging in.

Overall, remember to be careful about what information you share online.



Top News Inside

- Three Most Common Phishing Scams
- Case Study: Feds Warn of New Scam On Seniors
- One and Done? Not with Ransomware!
- Case Study: MGM Resorts

Add more layers of cybersecurity to YOUR online activity! Visit us at **www.oasis.tech** or give us a call at **405.948.6500**

Three Most Common Phishing Scams

Phishing scams are attempts to trick you into revealing your personal information, such as passwords, credit card numbers, or Social Security numbers.

Scammers often send emails or text messages that appear to be from legitimate companies, such as banks, credit card companies, or government agencies. They may also create fake websites that look like real websites.

The most common phishing scams are...

1. **Fake shopping websites**, which sell counterfeit products–or even sell nothing at all.
2. **Romance scams** to trick people into falling in love, so they'll be more willing to send money.
3. **Social media scams** that either impersonate real people, or invent new personas entirely.

Other common internet scams include:

- Investment scams that promise victims high returns on their investments, but the investments are actually fake.
- Tech support scams which claim to be a tech support company, but then charge for unnecessary services or steal personal information.
- Lottery and sweepstakes scams tell people that they have won a lottery or sweepstakes, but they need to pay a fee to claim their prize.
- Charity scams impersonate legitimate charities and ask for donations.

If you receive an email, text, or call from someone who is asking for your personal information or money, **be suspicious!** Don't click on anything until you verify the sender is who they say they are!

Did you know? **3.4B phishing emails are sent every single day!** For context, there are only 8B people in the world. Considering not all of them are on the web, **that's a huge chunk of the world left as a target!** It's important to know how to recognize and respond to phishing threats out in the wild, so you can keep your data protected!

Case Study: Feds Warn of Scam On Seniors

Senior citizens are no stranger to cyber-danger. They're infamously painted as technologically naive. Whether that's true or not, you SHOULD be aware of certain cyber-scams that are targeting an older demographic.

Recently, the FBI warned of a "phantom hacker" after nearly 20K reports came in about a threat group posing as the government and warning seniors that their finances had been hacked. The threat actors then directed their targets to transfer their money into a "safe" government account.

Remember...legitimate organizations, especially the government, will NEVER ask you to send money over the phone, or indeed anywhere except for a secure, online government portal.

Be very careful when receiving any suspicious requests for money or information. Vishing, or voice phishing, happens over the phone; Smishing happens over SMS messages; traditional phishing takes place on the phone.

Don't send money or information to anyone you don't know! If you're not sure if a request is legitimate, go to the government website and investigate further.

Case Study: MGM Resorts

Ever stayed at MGM Resorts International? If you weren't at one of their 30 international hotel, resort and gaming venues in September, then you should be grateful!

A threat group called Scattered Spider has claimed responsibility for the attack; they are known for using social engineering techniques to trick employees into granting the hackers access to large corporate networks. They operate underneath a well-known ransomware gang, ALPHV, who also go by the name "Black Cat."

The ruse was uncomfortably simple: They group just went on LinkedIn and discovered somebody who worked in the company's IT department as a legitimate employee. Then, they called the MGM help desk and saying they had been locked out of their account, asking for re-access.

The attack affected MGM's ATMs, slot machines, digital room keys and other digital payment systems, which all went offline during the attack. The company's corporate email, restaurant reservation and hotel booking systems also remained dark.

Ransomware attacks have become increasingly common in recent years, and they have targeted a wide range of organizations, including businesses, governments and healthcare providers all around the world.

One and Done? Not with Ransomware!

If you've had any amount of security awareness training, you should know that ransomware poses a very serious threat to your bank account and file security...to say nothing of your reputation with the customers whose PII you manage!

Did you know, though, that **ransomware also has long-term effects that can haunt you long after the initial attack?**

First of all, let's consider the personal cost that accompanies a data leak. If you don't pay the threat actor (or even if you do, because they frequently renege on their promise to leave your data alone) then they can publish that information on the Dark Web.

That means possible years of your PII being mishandled and abused, and **can have the domino effect of exposing you to even more cyber-threats later on.**

Furthermore, the recovery costs associated with ransomware can climb into the millions – even just to get business back to its usual pace.

As cybercriminals get savvier, **security experts are working even harder to bring you stronger and more efficient defenses.** Just knowing what to look out for online and staying aware of the latest trends and threats on the horizon will help you make safer decisions while you're browsing the web.