DECEMBER 2023 ISSUE NEWSLETTER - OASIS TECHNOLOGIES

KEEP THE HOLIDAYS HAPPY WITH CYBERSAFETY AND COMPLIANCE!

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!

Top News Inside

- Why Reporting Matters in a Data Breach
- Crash Course in Mobile Scams
- Top 3 Security Threats That YOU Should Know About

Cyber-Compliance is Serious Business

If you've never experienced a cyberattack, you might not think it's such a big deal. Especially if you work in management, you're so busy focusing on the so-called squeaky wheels of every day; does it really matter if you keep up with the intricacies of modern cybersecurity compliance protocol?

YES!

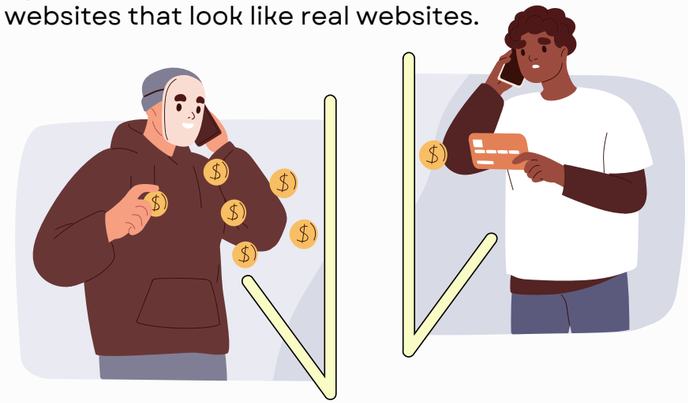
Increased digitization across the globe plus ever-advancing cyber threats equals a constantly evolving market, and legislation that scrambles to keep up!

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

Top 3 Security Threats That YOU Should Know About

Are you brushed up on your Phishing Training? If not, then you really should be!

Phishing scams trick you into revealing your personal information, like passwords, credit card numbers or Social Security numbers. Scammers send 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.



1. Fake shopping websites sell counterfeit products, or none at all. They often have low prices and free shipping to attract customers. Once you place an order, you may receive a fake product, no product at all, and your credit card information may be stolen too!

2. Romance scams trick people into falling in love with them…just to steal their money. Scammers often create fake profiles on dating websites and social media to gain their victim's trust; thereafter they'll ask for information or money, such as to help them with a financial emergency or to pay for travel expenses to "meet up."

3. Fake social media accounts may be entirely made up, or impersonate real people. The catfish behind the fake page may also send spam messages or post links to malicious websites.

Crash Course in Mobile Scams

How often do you use your mobile device?

If you're like the average American, you check your phone nearly 150 times per day. That alone makes mobile scams a very serious and real threat!

So, what should you be on the lookout for?

Even if you don't check your email on your phone, you could still be a victim of **phishing** attempts.

Have you ever gotten a robocall threatening you with legal action from the IRS or DMV? **Vishing** is voice phishing that happens via telephone call.

Smishing attempts reach out via SMS message, more commonly known as texting.

It's not only phishing you should worry about. Scammers sometimes create fake apps that look like real apps, but steal your data when you open them. Only ever download from trusted app sources and stores!

No matter what avenue these phishers take, the end goal is the same: Convince their target to download malware or reveal personal information. Know the threats lurking on your mobile device, so you can stay safer every time you check your phone.

THE MORE YOU KNOW

Did You Know?

An estimated 2,200 cyberattacks are launched every day.

If it happens to *you*, then you could be found guilty of noncompliance!

If your organization manages customer PII, then you are *legally obligated to comply* with cybersecurity laws that depend on your location, industry and job role.

Why Reporting Matters in a Data Breach

Have you ever experienced a cyberattack, either aimed at you or leveled at your organization?

If so, then you might already know how important it is to report the breach…and we don't just mean to your direct managers or the police!

When a data breach happens, you are often beholden to laws detailing what, how fast and to whom you must disclose. For example, **financial institutions have to notify the Federal Trade Commission within thirty days**. You typically have to disclose the breach to anyone affected, too, depending on what information was stolen.

Where do you work? **Do you know the laws set upon your industry and role?**

So not only does cyber-compliance affect your ability to protect yourself and your customers from a data breach, but that hack will affect customers' trust in your ability to keep their personal and financial information safe.

Consider that the average company spends $10K per employee on cyber-compliance, and you see why maintaining compliance saves millions – about half of what you'd spend if you let vulnerabilities lay rampantly unpatched!

Maintaining compliance isn't just smart; it's necessary. To foster good relationships with your customers and shareholders, and avoid fines and breaches, companies must maintain a compliant cybersecurity structure. These regulations change over time but do so to keep up with the latest tricks up cybercriminals' sleeves.

Our IT services include compliance as part of our all-in-one package, to reduce excess labor on your end. **We'll stay up to date on changing regulations so you stay cyber-compliant!** Reporting is one of many important regulations that make you more cyber-secure!

Think about it: If your bank accounts, or health records, or mailing information got leaked, wouldn't you want to know? It's not just about preferences, though…data privacy is a right in many countries across the globe!

How can we keep our accounts and data private if we don't know when a breach has occurred? If you don't know YOUR reporting requirements, now is the time to found out!