ANYWAY TECH
LEADING THE COMMUNITY

205 MERRIMAN AVE
WYNNE, AR 72396

Top News Inside

Is TikTok on the Way Out?

TikTok is one of the most famous — or depending on your view on the matter, infamous — applications out there.

From privacy suits to serious legal discussions about data collection, TikTok has been subject to a lot of talk since it became the most downloaded app back in the tail-end of 2018.

Now more bans seem to be in the works for the social media app.

Some U.S. states are drafting or debating banning TikTok right now.

India has already banned the app nationwide.

Australia, Belgium, the Netherlands and France are just a few other countries that have already set regulations for the platform.

Why are people so concerned about TikTok, even more so than other social media apps? After all, *most* social media collect lots of data on their users!

Well, everyone's reasons for being especially wary of TikTok vary. Maybe you've heard some of these concerns before:

- TikTok tends to attract a younger age demographic, which particularly concerns parents and guardians of Gen Z
- The video-based platform naturally creates concerns about users' **digital footprint**
- Some fear national security concerns related to international data collection
- In general, mass data collection concerns citizens who don't live under strict privacy laws, and who may not want that much of their personal data saved

Monthly
Newsletter
September 2023 Issue #27

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!

HAVE A SAFE YEAR STUDENTS!

Bringing you the monthly scoop on information security.

From the tricks hackers are using against you right now, to the best digital defenses available, to small ways you can protect your accounts every day, we're here to bring you up-to-date news on cyber-safety!

"Granted, we haven't finished a single project either."

THE MORE YOU KNOW

Did You Know?

Almost 60% of people around the world have some form of social media.

Because social engineering threats continue to run rampant, you need to be careful of who you're talking to, sending information to, or even meeting up with online!

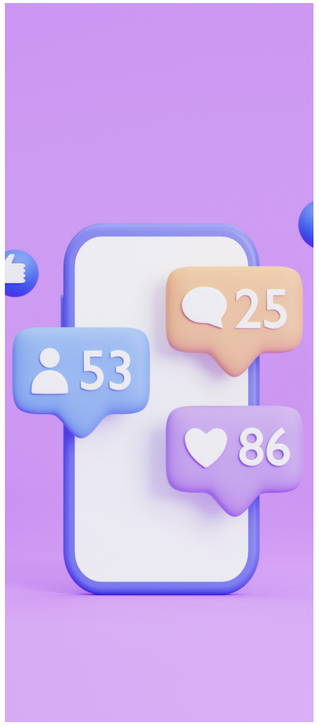
Then there's the matter of data privacy. How much information does your favorite social media platform collect about YOU?

Are You Using Social Media Securely?

Social media is a great tool for your organization's communication and engagement!

A business profile can provide real-time information to clients, connect directly with your target audience, and perhaps most importantly, humanize your organization. Consumers can get to know your brand and the people behind it, and vice versa.

Privacy and security risks associated with social media platforms only increase as the number of users and platforms grow. Cybercriminals mine social media accounts to get valuable intelligence that they can use in malicious campaigns. All organizations should develop a social media policy.



These profiles must be secured.

Review your social media policy at least once per quarter!

Go over the privacy settings for each platform and make any necessary changes. Make sure only the people who need access and publishing privileges have them, remove anyone who does not, and change privileges as needed.

The first step is to develop a social media policy that includes what can be posted, who can post, and on what devices (e.g., can they use their personal device, or does it have to be a company-owned device?), and who is responsible for keeping and changing passwords.

These are just some of the things that need to be addressed!

- Establish a social media team headed by a senior person
- Insulate employees who choose to participate in your social media campaign; don't link company and personal accounts
- Use role-based email addresses instead of employee emails, i.e. social@company.com or communications@company.com
- Don't post photos in front of workspaces; you may accidentally photograph confidential information at someone's desk
- Consider a policy of zero trust and require that all posts be vetted by the social media team for content prior to publishing

3 Unexpected Places We Risk Online Security

The Internet has pervaded nearly every activity we do. Whether we're watching our Smart TVs or networking with people on the other side of the world, so much of our daily lives are spent online that we barely think about it anymore!

Have a question? Jump on your favorite search engine. Need to impress friends with an obscure fact? Find scholarly articles in just a few clicks. Want to see a movie, or request time off, or plan a date in a new neighborhood, or find a new job? Online, online, online.

Our whole lives are digital now. Take these 3 steps to better protect yourself on the Internet!

1. **Avoid public WiFi.** Even if the guest WiFi is password-protected, you never know who's logged in and spying on everything you do.

2. **Don't post your every move on social media**. The more you tell about yourself online, the more a hacker can learn about you before launching a social engineering scheme or using that knowledge to hack your account.

3. **Don't use IoT devices on networks** that hold important data. IoT devices are notoriously easy to break into, making it a good gateway into your network!

Everything You Need to Know About PII

How much do you really know about this important term, and keeping *your* PII secure on a daily basis?

PII stands for *personally identifiable information* and encompasses data that can be tied back to who you are, specifically. Things like your name, home address, phone number and Social Security number are all different types of PII.

All PII, regardless of how easy it is to tie back to you, must be protected.

It is considered confidential, protected data and those you manage it must do their best to safeguard it in storage and transit alike. This may sound intuitive, but classifying it as protected information allows the government to construct best practices and audit systems to guarantee your data's safety, as well as outline punishment for violations.

- PII is also the most expensive data that can be compromised in a breach, as the hacker could sell it, break into and buy goods off of your accounts, and even extort the victim directly

- PII is the most commonly compromised kind of data, encompassing 44% of cyberattacks

- Criminals can sell your private information for hundreds of dollars on the Dark Web, selling for an average of about $200 per record

- In 2021, breaches that compromised credentials cost a total of over $4M

Cybercriminals often go directly after master vaults of PII, like using a company's sales database against them; this is why it's important to use different credentials across all of your various accounts. The loss or compromise of one password shouldn't mean the destruction of your entire online presence.

Keep your private data secure, whether you're communicating it online or have the files safely in storage. Education and vigilance is the best way to stay cyber-secure every day!

Protect Your PHI: Breaking Down Private Health Information

We've all go to the doctor. Maybe you make frequent trips for a chronic illness, or do regular checkups as needed.

When you pass along information like your name, medical background and credit cards, you give what's known as ***protected health information***.

Maintaining privacy in the modern world requires a lot of regulation. Even prescriptions can be acquired through video-chat these days!

Knowing your privacy rights helps you enforce ALL of your digital and physical data boundaries more comfortably. The better you understand your PHI, the better you can manage it!

Unfortunately, healthcare providers are not insulated practices.

They work with manufacturers, associates and suppliers that must sometimes access the healthcare provider's internal network. Any of them could acquire a malware infection that spreads when they log onto the local WiFi, or get phished for their account credentials. ***You see how quickly that could spell trouble for the healthcare provider – and all their patients!***

Thankfully, healthcare providers are required to report big breaches within 60 days of their discovery, so it's not as though you won't know an incident has taken place. ***Encrypt your digital communications, use complex passwords, set up multi-factor authentication and set strict permissions*** to help keep your protected health information as secure as you can.

Dig into your various healthcare providers to make more informed decisions about who you trust to handle *your* PHI!