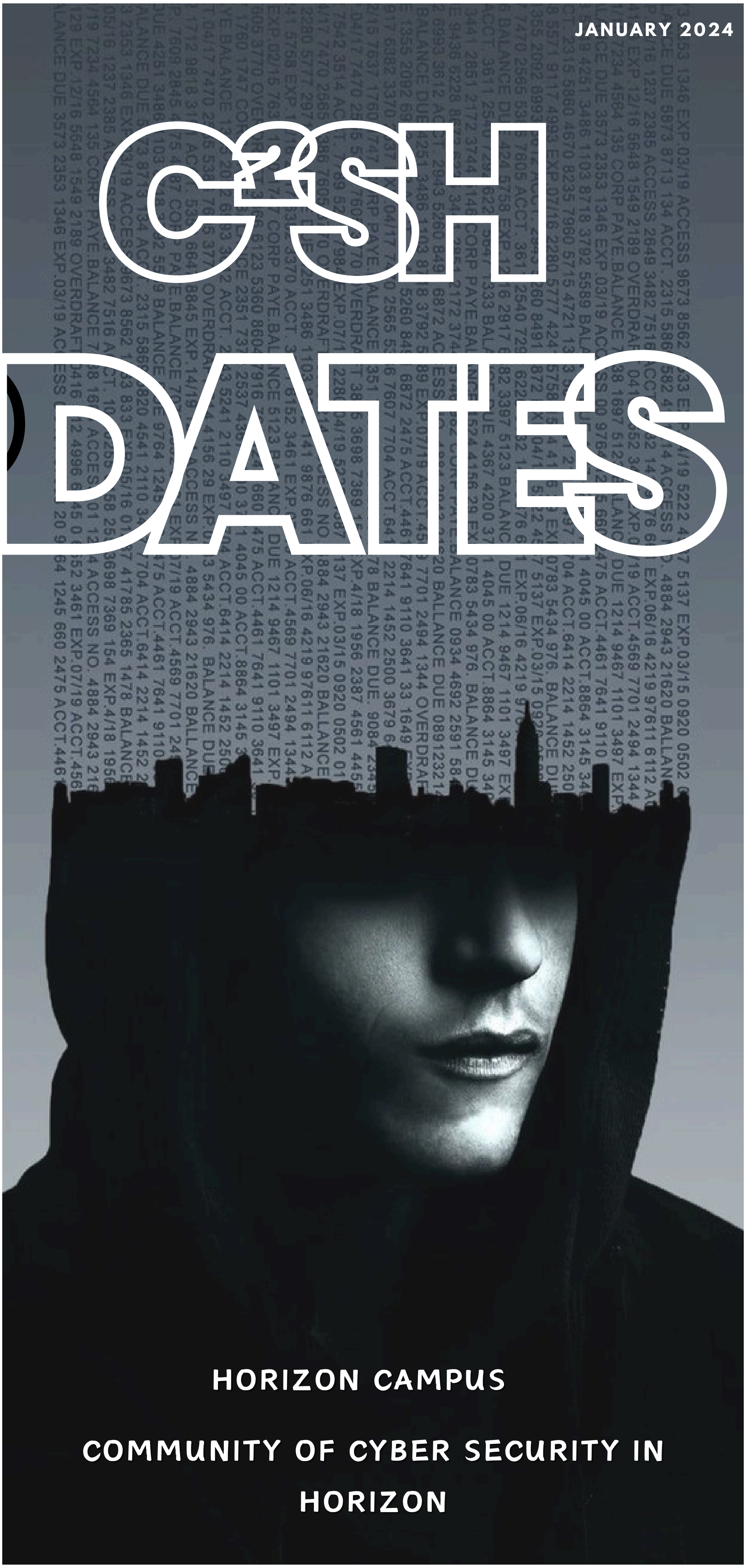
EDITION #02

JANUARY 2024

C^{3}SH UPDATES



NAVIGATING THE SOCIAL MEDIA LANDSCAPE: A GUIDE TO CYBERSECURITY

NAVIGATING THE SOCIAL MEDIA LANDSCAPE REQUIRES A PROACTIVE APPROACH TO CYBERSECURITY. BY IMPLEMENTING THE PRACTICES HERE AND BEING AWARE OF EMERGING THREATS, WE CAN ENJOY THE BENEFITS OF SOCIAL MEDIA WHILE PROTECTING OUR DIGITAL WELL-BEING.

REMEMBER, YOUR ONLINE SECURITY IS IN YOUR HANDS. STAY SAFE, STAY INFORMED, AND ENJOY YOUR DIGITAL EXPERIENCES RESPONSIBLY.

HORIZON CAMPUS

COMMUNITY OF CYBER SECURITY IN HORIZON

NAVIGATING THE SOCIAL MEDIA LANDSCAPE: A GUIDE TO CYBERSECURITY

In the age of social media ubiquity, where our digital lives intertwine with the virtual realms of platforms like Facebook, Twitter, and Instagram, the need for cybersecurity awareness has never been more critical. This article aims to serve as a guide, empowering users to protect themselves in the dynamic and sometimes treacherous landscape of social media.

1. FORTIFY YOUR PASSWORDS:

A robust password is your digital fortress, protecting your personal information from unauthorized access. Consider the following tips to enhance the strength of your passwords:

Passphrase Power

- Opt for passphrases over single-word passwords. A passphrase is a sequence of words or a sentence, making it harder for attackers to crack.
- Use a combination of unrelated words or a memorable sentence to create a passphrase. For example, **"Horizon@Campus2024."**

Avoid Common Patterns

- Steer clear of easily guessable patterns, such as "123456" or "password." Cybercriminals often exploit these common choices first.

- Avoid using easily accessible personal information, like birthdays or names, as part of your password.

Mix and Match

- Integrate a mix of uppercase and lowercase letters, numbers, and special characters in your password. This complexity adds an extra layer of defense against brute-force attacks.

- Consider substituting letters with similar-looking characters or numbers, such as replacing "O" with "0" or "E" with "3."

Password Length Matters

- Aim for longer passwords. The more characters your password contains, the more resistant it is to cracking attempts.

- Many cybersecurity experts recommend a minimum password length of 12 characters or more.

Unique for Every Platform

- Avoid the common pitfall of using the same password across multiple platforms. If one account is compromised, using unique passwords ensures that other accounts remain secure.

- Consider employing a password manager to generate and store complex, unique passwords for each platform.

Regular Password Updates

- Periodically change your passwords, even if there's no indication of a security breach. Regular updates mitigate the risk of prolonged unauthorized access.

- Use calendar reminders or built-in features of password managers to prompt password changes every few months.

Enable Two-Factor Authentication (2FA)

Add an extra layer of security by enabling Two-Factor Authentication. This typically involves receiving a code on your mobile device that you must enter alongside your password. This additional step significantly enhances the security of your social media accounts.

2. BE MINDFUL OF PRIVACY SETTINGS

In the vast and interconnected landscape of social media, your privacy settings act as the virtual gatekeepers of your personal information. Consider the following details to ensure a nuanced and customized approach to your social media privacy

Profile Visibility

Review who can see your profile information. Social media platforms typically offer options such as "Public," "Friends Only," or "Custom." Assess which setting aligns with your desired level of visibility.

Customize your profile visibility based on the nature of the platform. For professional networks like LinkedIn, you might prefer a more open profile, while on personal platforms, limiting visibility may be a priority.

Post Audience

Take control of who sees your posts by adjusting the audience settings for each individual post. Options often include "Public," "Friends," "Only Me," or custom lists.
Before posting, evaluate the sensitivity of the content and tailor the audience accordingly. Consider creating friend lists for more granular control over post visibility.

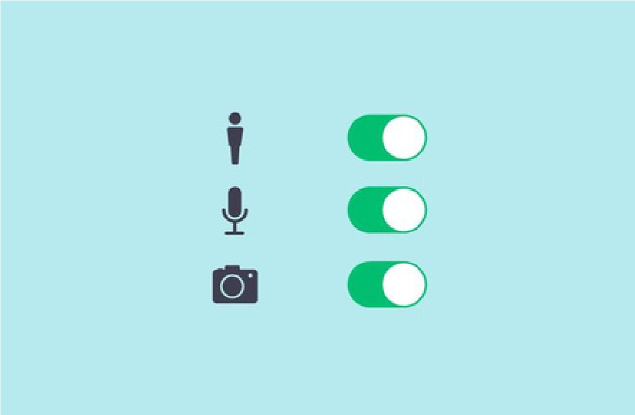
Tagging Permissions

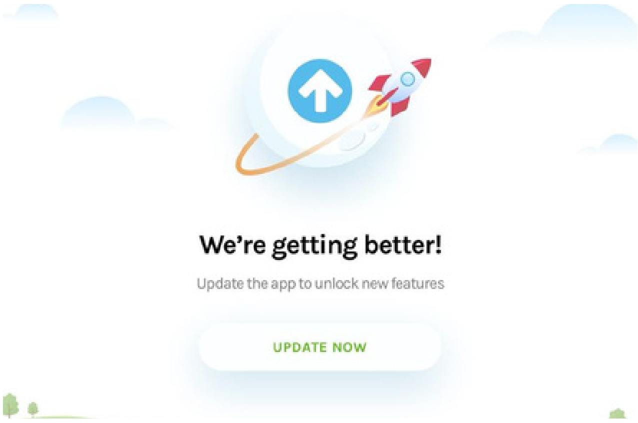
Manage who can tag you in posts and photos. Some platforms allow you to review tags before they appear on your profile, providing an added layer of control.
Adjust settings to ensure that only friends or specific groups can tag you. This minimizes the risk of being tagged in content that may compromise your privacy or professional image.

App Permissions

Review and manage third-party app permissions connected to your social media accounts. Some apps may request access to your profile information or friends list.

Remove access to apps that you no longer use or trust, reducing the potential for unauthorized data collection.





We're getting better!

Update the app to unlock new features

Check Platform Updates

Social media platforms frequently update their features and privacy settings. Stay informed about these changes and revisit your privacy settings accordingly.

Subscribe to platform newsletters or follow official social media accounts for announcements about new features or changes in privacy policies.

3. THINK BEFORE YOU CLICK

1. Scrutinize Social Media Direct Messages

Be especially vigilant when clicking on links received through direct messages on social media platforms. Phishing attacks often target individuals through seemingly harmless messages, which may contain malicious links. Verify the sender's identity, even if the message appears to be from someone in your network.

2. Beware of Clickbait Content

Social media platforms are rife with clickbait content designed to lure users into clicking on intriguing links. Exercise skepticism when encountering sensationalized headlines or offers that seem too good to be true. Verify the legitimacy of such content before clicking..

3. Hover Over Links to Preview

Hover your cursor over a link without clicking to preview the actual URL. This simple action can reveal whether the link redirects to a suspicious or unfamiliar website. Avoid clicking on links that have unexpected or complex URLs.

4. Check URL Legitimacy

Before clicking on a link, carefully inspect the URL. Phishers often use misspelled or slightly altered URLs to imitate legitimate websites. Ensure that the domain matches the official website and watch for subtle variations.

5. Verify Shared Content with Friends

If you receive unexpected links from friends, especially if the content seems out of character or unusual, take a moment to verify with the friend directly. Their account might have been compromised, and the link could be part of a phishing attempt.

6. Be Cautious of URL Shorteners

Exercise caution with shortened URLs, commonly used on platforms like Twitter(X). While they can be convenient, they obscure the actual destination. Consider using URL expander tools to preview the full URL before clicking.

7. Educate Yourself on Social Engineering Tactics

Stay informed about social engineering tactics employed on social media platforms. Cybercriminals may impersonate friends, family, or trusted entities to trick users into clicking on malicious links. Be skeptical of unexpected messages, especially those urging immediate action.

8. Enable Security Features

Utilize security features offered by social media platforms. For instance, Facebook provides a "Trusted Contacts" feature, which adds an extra layer of protection for account recovery. Familiarize yourself with these features and enable them for added security.

4. BE WARY OF OVER-SHARING

Consider Audience Appropriateness

Before sharing personal information, consider the appropriateness of your audience. Different platforms allow you to customize the audience for each post. Tailor your sharing based on whether the content is intended for friends, family, or a broader public audience.

Limit Location Sharing

Exercise caution when sharing your location in real-time. While it can be fun to check in at a favorite restaurant, constant location sharing may expose patterns of your daily life. Be selective in sharing location information and disable location settings for apps that don't require it.

Educate Yourself on Geo-Tagging

Understand the implications of geo-tagging in photos. Some social media platforms automatically attach location data to your posts. Disable this feature if you're uncomfortable with the idea of your exact location being visible in every post.

Avoid Public Displays of Personal Documents

Refrain from sharing personal documents, such as IDs, passports, or credit cards, even in a celebratory context. These documents contain sensitive information that can be exploited by cybercriminals for identity theft.

Think Twice Before Sharing Personal Achievements

While it's natural to share accomplishments, be mindful of oversharing personal achievements that might inadvertently expose details like your full name, workplace, or other identifiable information. Celebrate success without compromising your security.

Mind Your Digital Footprint

Remember that every post contributes to your digital footprint. Even seemingly innocuous information, when aggregated, can create a comprehensive profile. Consider the long-term implications of what you share online.

Limit Details in Public Profiles

Be selective about the information you include in your public profile. Avoid including sensitive details such as your full birthdate, address, or phone number in publicly visible sections. Reserve such details for private or restricted settings.

Regularly Audit Your Posts

Periodically review your past posts and content. Remove or update any information that you no longer wish to be publicly accessible. Consider it a digital spring cleaning to ensure your online presence aligns with your current preferences.

5. EDUCATE YOURSELF ON SOCIAL ENGINEERING

Understanding Spear Phishing

Be aware of spear phishing, a targeted form of phishing where cybercriminals tailor their messages to a specific individual or organization. These messages may appear highly personalized and convincing, often using information gathered from social media or other online sources.

Pharming and Pharming Attacks

Familiarize yourself with pharming attacks where attackers redirect users to fraudulent websites without their knowledge. Cybercriminals exploit vulnerabilities in DNS or manipulate hosts files to redirect users to malicious sites, often indistinguishable from legitimate ones.

Recognizing Impersonation Tactics

Develop an eye for recognizing impersonation attempts. Cybercriminals may pose as colleagues, friends, or even official entities. Scrutinize messages and requests for any anomalies or unusual behavior that deviates from the person's typical communication style.

Beware of Fake Customer Support Calls

Be cautious of unsolicited calls claiming to be from customer support, government agencies, or tech support. Legitimate organizations typically do not request sensitive information or payment details over the phone. Hang up and independently verify the caller's identity.

Verification of Emergency Scenarios

In the face of urgent or emergency scenarios presented online, take a step back. Cybercriminals often exploit a sense of urgency or fear to manipulate users. Verify the authenticity of such messages through official channels or contacts before taking any action.

Spotting Emotional Manipulation

Recognize emotional manipulation tactics used by cybercriminals. They may craft messages to evoke fear, sympathy, or excitement to prompt immediate action. Pause and assess the emotional tone of messages, and be skeptical of requests that leverage strong emotions.

Check for Typos and Inconsistencies

Pay attention to spelling and grammar in messages. Phishing attempts often contain typos or linguistic inconsistencies. Genuine communication from reputable sources is typically well-crafted and free of such errors.

Verify Email Sender Addresses

Verify the authenticity of email sender addresses. Cybercriminals often use email spoofing to mimic legitimate email addresses. Check for subtle variations or misspellings that may indicate a fraudulent email.

Stay Informed About Current Tactics

Stay informed about the latest social engineering tactics. Cybercriminals continually evolve their methods, and awareness of current trends enables you to recognize and thwart emerging threats effectively.