Safe & Sound

Brought to you by
Wintek Powered by Tipmont

Tips to Share with Care on Social Media

BY WINTEK

Social media lets you amplify your attitude, promote your passions and champion your creativity. Maybe you'll create the next TikTok dance craze. Perhaps your path to Instagram-influencer fame starts today.

There's no speedier way to share your social media updates than using Wintek's blazing-fast fiber connection, whether it's available in your apartment or at one of our free public WiFi hotspots.

But don't always be so quick to click. Always assume anything you post online will live forever in backups and screenshots. The last thing you want is for a careless comment or provocative post to harm you or someone close to you in the future.

Before you post or comment, ask yourself the following questions:

• Does what I'm saying or showing reflect who I truly am?

• Could this create issues for me later?

• Would I be OK with a potential employer seeing / reading this?

• Could this pose problems for someone else?

Here are some additional tips to keep in mind so you can share with care when using social media:

• Never share sexually explicit content that concerns you or anyone else.

• Avoid inappropriate, hateful or harmful comments. In other words, don't be a troll.

• Set your profiles to private where possible and limit your interactions to people you know and trust.

• Never assume that your privacy settings offer perfect protection. Always think before you post.

• Use caution with potentially controversial opinions, even in private groups or among friends.

• Don't use potentially embarrassing or inappropriate handles or screen names.

• Verify that any news articles you share are verified or come from a trustworthy source.

When TMI takes a turn

How to avoid online sharing pitfalls

BY JILLIAN ELLISON
Exponent Advertising Department

Social media can help us keep in touch with old friends in the present while reminiscing on the past, but security professionals advise to be wary of what all you share on your personal pages.

Oversharing your life on social media and answering the fun polls frequently shared across Facebook can cost you more just the time it took to think of the answer.

Kathryn Seigfried-Spellar, an associate professor in the Department of Computer and Information Technology at Purdue, said answers to those popular polls are often security questions that are asked when logging into your bank's website and other sensitive accounts.

"Those answers to questions can often be used to guess passwords as well," Seigfried-Spellar said, "which is something you want to avoid altogether."

An online predator isn't always a stranger either, Seigfried-Spellar said. It's crucial to remember that those you've connected with on social media aren't always just there to see you through life's moments.

"When you overshare that you're currently out of town at a particular place, that's a great opportunity for someone looking to break and enter and steal valuables," she said. "If you're in Europe and posting about it, I can take that as an opportunity to call loved ones and create the scenario that you've lost your wallet or passport and I'm trying to crowd fund for you to get the situation fixed."

Nicknames only family call you are bound to slip out eventually, Seigfried-Spellar said, and being able to call you by that name creates a more believable situation when the predator is talking to family to try to scam them.

Though you may have a lot of "friends" on social, not everyone is on social media to be your friend. The National Cybersecurity Alliance recommends using the tools offered from platforms such as Facebook to limit and manage who on your friends list is able to see certain information listed in your profile. Creating lists of close friends and limiting who can see particular posts will limit the eyes on your sensitive information.

Targeting less-than-private accounts is a simple way for hackers to obtain information. Seigfried-Spellar said she recommends turning on privacy settings to limit who can see what's going on in your life. But even taking these steps can only provide so much protection.

"Information about you can be gathered from other people as well," she said. "Your parents and friends are sharing things about you even if your privacy settings are all the way up. No one wants to read the terms and conditions for social media pages, but once you post something, that is now owned by that platform. When you use social media, your information is being sold, and whether or not you're fine with that is a personal decision you have to make."

Cybercrime on campus: tips to stay safe from scammers

BY STACEY KELLOGG
Exponent Advertising Department

Catfish have gotten a bad rap in the last few years. The whiskered bottom feeder's namesake is now associated with some of the world's most notorious types of crimes: cybercrimes where people are scammed by those pretending to be someone else.

Catfishing is the term used to describe when someone deceptively creates a fake online persona to dupe someone out of money, assets, their identity, and/or sex. In most cases, catfishing cases involve some kind of prolonged romance scam, whereby the catfisher gains the romantic trust of the person being scammed.

Even though America has capitalized on the concept with "Catfish: The TV Show" (as America does) and created awareness around the topic, victims continue to fall prey to this and other electronic and cybercrimes. Purdue students, faculty, staff, and the greater West Lafayette community are no exception.

According to the Purdue University Police Department (PUPD), fraud reports encompassing a wide spectrum of behavior have affected campus increasingly over the last five years. Between 2017 and 2018, fraud reports to PUPD nearly doubled from 28 to 54. In 2019, reports took a tip to 40, but ramped up again to 54 in 2020. To date (Sept. 14, 2021) PUPD has received 18 reports of fraud.

These numbers encompass all fraud reports, including but not limited to fictitious border enforcement officers threatening to deport victims, part-time job offer email scams, never receiving goods paid for via online marketplaces, and identity fraud and theft, according to Song Kang, PUPD's captain of special services.

PUPD Police Chief John Cox said internet fraud is the most-often reported digital crime.

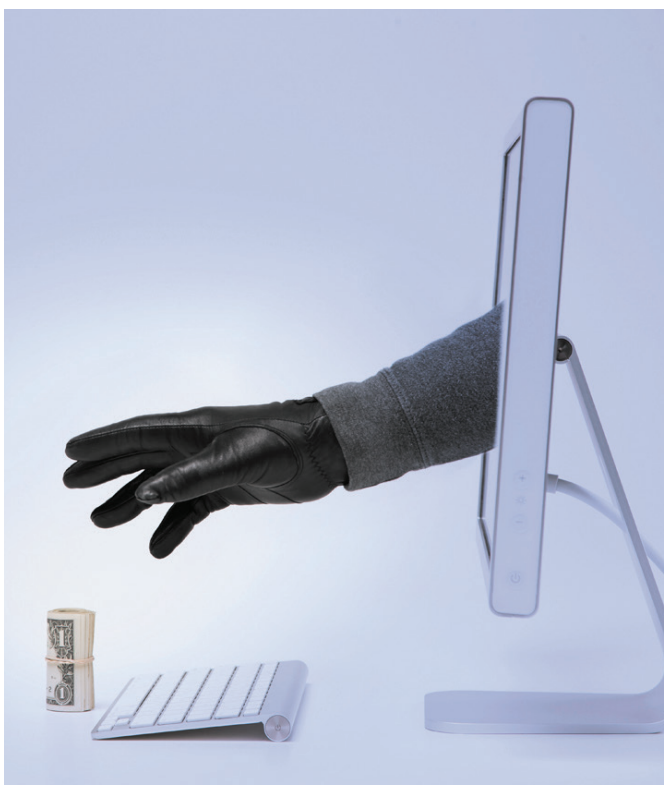
"Both domestic and international students are victimized every semester," Cox said. "The best thing to do is to never give out your personal information or agree to some sort of money wire or transfer from someone you do not personally know and can verify. Always report suspicious activity to police," he said.

The key words here - someone you personally know – can get blurry when concepts like catfishing and phishing are at play. Those who fall victim to catfishers feel like they do know their scammers. Before giving any money or your bank account information to anyone, listen to your instincts. According to WebMD, here are some ways to spot someone who might be catfishing:

1) They avoid showing their face while communicating

2) Their social accounts don't have many friends or interactions, and profile pictures seem fake

3) Their stories are too good to be true, and their tragedies for which they need money are over the top



4) They ask for money

5) They are extremely romantic right away (also called love bombing)

Phishing emails and calls – whereby you receive an email that appears to be from someone you know, or emails that appear to be from official sources – are effective in getting people to act. Usually there is some sort of threat: The IRS is coming after you so you need to verify your bank information, or your computer has been compromised and you need to send money to fix it. Many successful scams involve scammers asking victims to purchase gift cards and send them the gift card numbers and codes right away.

To reduce the chances of being victims of these situations, never click on links in emails unless you know for sure someone you know is sending you a link to explore. Look for spelling errors or sentences that seem as if they are not complete or contain broken English. Don't answer phone calls from unknown numbers. Don't answer or return calls from robo-callers. If you think the voicemail is legitimate, contact the company using a phone number you already have on file on your own to see if they have been trying to reach you.

"Our standard advice is: do not click on anything or agree to do anything from anyone online unless you know the site or person to be authentic. Always check with your local police department and report suspicious activity or victimization right away," Cox said.

To be proactive, PUPD, Information Technology at Purdue (ITaP) and other university departments provide training on how to avoid online scams.

"We work directly with ITaP security when new scams pop up and then educate the community through news releases to the media. We also connect victims of these crimes with support services and information so they know what the next steps are in recovering their money or identities," Cox said.

According to the PUPD website, individuals who believe they may have been a victim of fraud should report it to the police department in the jurisdiction in which the crime took place. Regardless of where you live, where the crime occurred is the determining factor of which police department to call for reports that do not require immediate police and/or medical response.

• If the crime occurred on the academic or residential portion of campus, contact the Purdue University Police Department at (765) 494-8221.

• If the crime occurred off-campus in the city of West Lafayette, contact the West Lafayette Police Department at (765) 775-5200.

• If the crime occurred in the city of Lafayette, contact the Lafayette Police Department at (765) 807-1200.

• If the crime occurred in Tippecanoe County, contact the Tippecanoe County Sheriff's Office at (765) 423-9388.

• The Indiana State Police Lafayette District 14 Office is available at (765) 567-2125 or 1-800-382-7537