

JOURNEY TOWARDS SECURITY

Stay secure while preparing for the new year



THIS MONTH'S TOPICS:

Resolutions

And how to stay secure...

Pop-Up Scams

The Past and Present...

Scam of the Month:

Social Media Lockout Scams...

The Monthly Mashup:

December Updates and Review...

The new year is upon us!

Whether you are posting pictures from the holidays on social media, creating a new year budget, or setting up that gifted smart TV, cybercriminals are finding ways to sneak their scams into these exciting times. As you take on whatever the new year throws at you, make sure your journey includes staying cyber secure.

In this month's newsletter, learn about resolution-related scams, the past and present of pop-up scams, and the one online service you should never pay for. Don't forget to check out the monthly mashup!



RESOLUTIONS

How to stay cyber secure while accomplishing them.

HEALTHY HABITS

There are many resources and programs online that can help you accomplish fitness and health goals. When searching for gyms, workout plans, or healthy recipes, watch out for scams. Some of these scams are just misleading ads, while others result in no product being delivered at all. Be wary of any pills, diets, or programs that promise immediate results.

NEW YEAR, NEW FINANCES

The new year is a great time to look at finances. With the rise of online shopping, it can be difficult to keep track of purchases. Set a routine to check your transactions on debit and credit cards and look for any suspicious charges you didn't make.

Many people are using budgeting apps. Make sure to read reviews and research the app before downloading or entering your personal information on it. Avoid entering your banking information on unknown apps.

QUICK CASH OR SCAM?

Online surveys may seem like an easy way to make money, but it is important to do your research before participating. Many of these sites are scams. If the money offered seems too high or if a reward is offered just for signing up, it is likely a scam. Be careful with your personal information. Read the privacy policy and leave the survey immediately if the questions ask for sensitive information.

POP-UP SCAMS

PAST AND PRESENT



Past

Pop-up ads have been a technique used by scammers for decades. By blocking the user's access to their screen with annoying pop-ups, there is a higher chance the user will purposefully or accidentally click on the malicious advertisement. These pop-ups could be advertising software updates, products, or hot topic articles. But these scams are not fully a thing of the past. It is important to still be cautious with any pop-ups as you browse today.

Present

Now scammers are taking their pop-ups to the big screen with smart TV pop-ups. Since many televisions are connected to the internet, scammers are creating pop-ups mimicking popular streaming services or other apps and claiming the user must pay their subscription fee or update their information. These pop-ups often include a website to visit or a phone number to call to fix the issue. This could lead to the scammer getting remote access to your TV, installing malware, or gaining access to your payment information and charging your card. Luckily there are many ways you can avoid falling for these scams.



Quick Tips

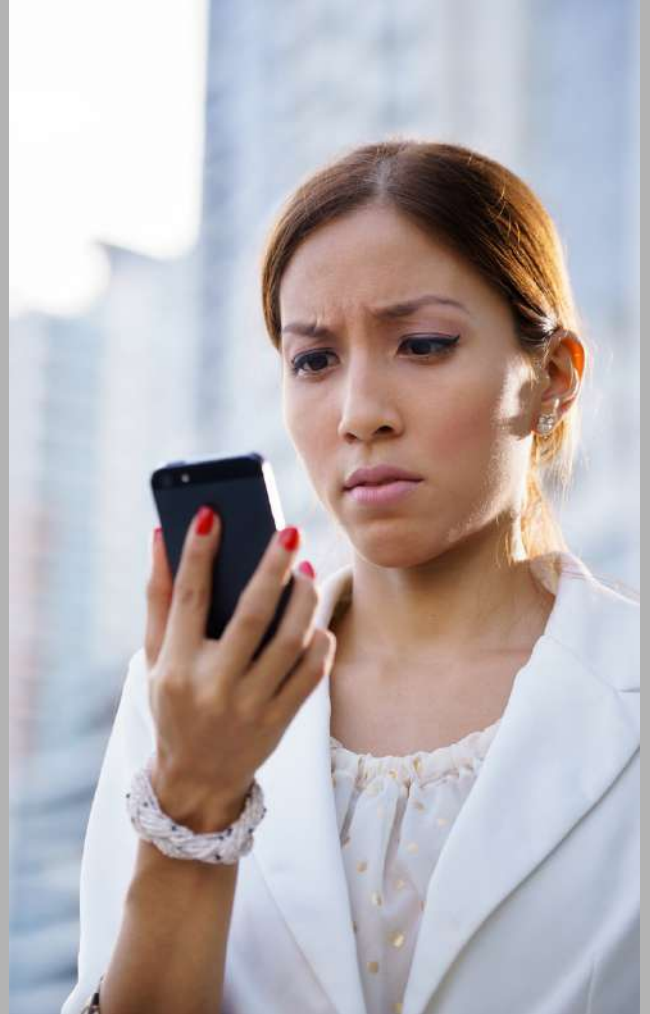
- Double-check the actual fees you have to pay on the official site.
- Don't let a stranger control your device remotely.
- Verify the URL or phone number on the screen first.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using **RIGHT NOW**, to better prepare you when the next scam hits.

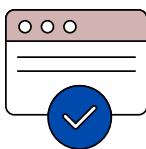
Ashley just got off work for the day. She opened her phone and clicked on her favorite social media app. She was eager to see what her friends and family were up to. But when the app opened, she had been logged out. She was locked out of her account. Desperate to regain access, she turned to the internet for help. She searched “how to recover my social media account” and came across a recovery company that promised to assist her for a fee. Ashley decided to give it a try and paid the requested fee.

As time went on, Ashley waited for her account to be recovered. She reached out to the company, and they asked for more personal information and an additional fee. Eventually, Ashley realized that the account recovery company was not going to be able to recover her account and that it was likely a scam. Ashley was correct. The company was fake. It was run by scammers posing as experts to gain access to user’s personal information and money.



Did you spot the red flags?

- ▶ Ashley should have researched the company first before paying the fee for their services.
- ▶ After the company requested more personal information and money, Ashley should have reported the company and the charges.
- ▶ Ashley should have reached out to the social media company directly instead of finding a third-party service.



Set up a second verification method like a recovery email or phone number so you can easily recover your account in this situation.



Never pay for social media account recovery services. The platform’s actual customer support channels will offer help for free.



These scams come in many forms. Scammers may reach out directly and claim your account has been hacked or that someone is making purchases on your account. Avoid third-party services offering recovery and go directly to the company website or customer service number.

THE MONTHLY MASHUP

KEY TAKEAWAYS

The new year is a great time to make goals and resolutions. Just remember, cybercriminals have their own resolution-related schemes they use to trick users.



JOKE OF THE MONTH

What did the password say after it got compromised on New Year's Eve?

New year, new me!

DECEMBER 31ST: NEW YEAR'S EVE

Stay up to date with cyber news and training to make sure you are prepared for whatever scams come your way this new year.

CYBER CROSSWORD

1. The new place scammers are using pop-ups.

2. It may seem like a good way to make quick cash, but it could lead to a scam or exposure of personal information.

3. You should never ___ for social media recovery services.

Final clue: What you should do before calling a phone number or clicking a link on an ad or pop-up.

