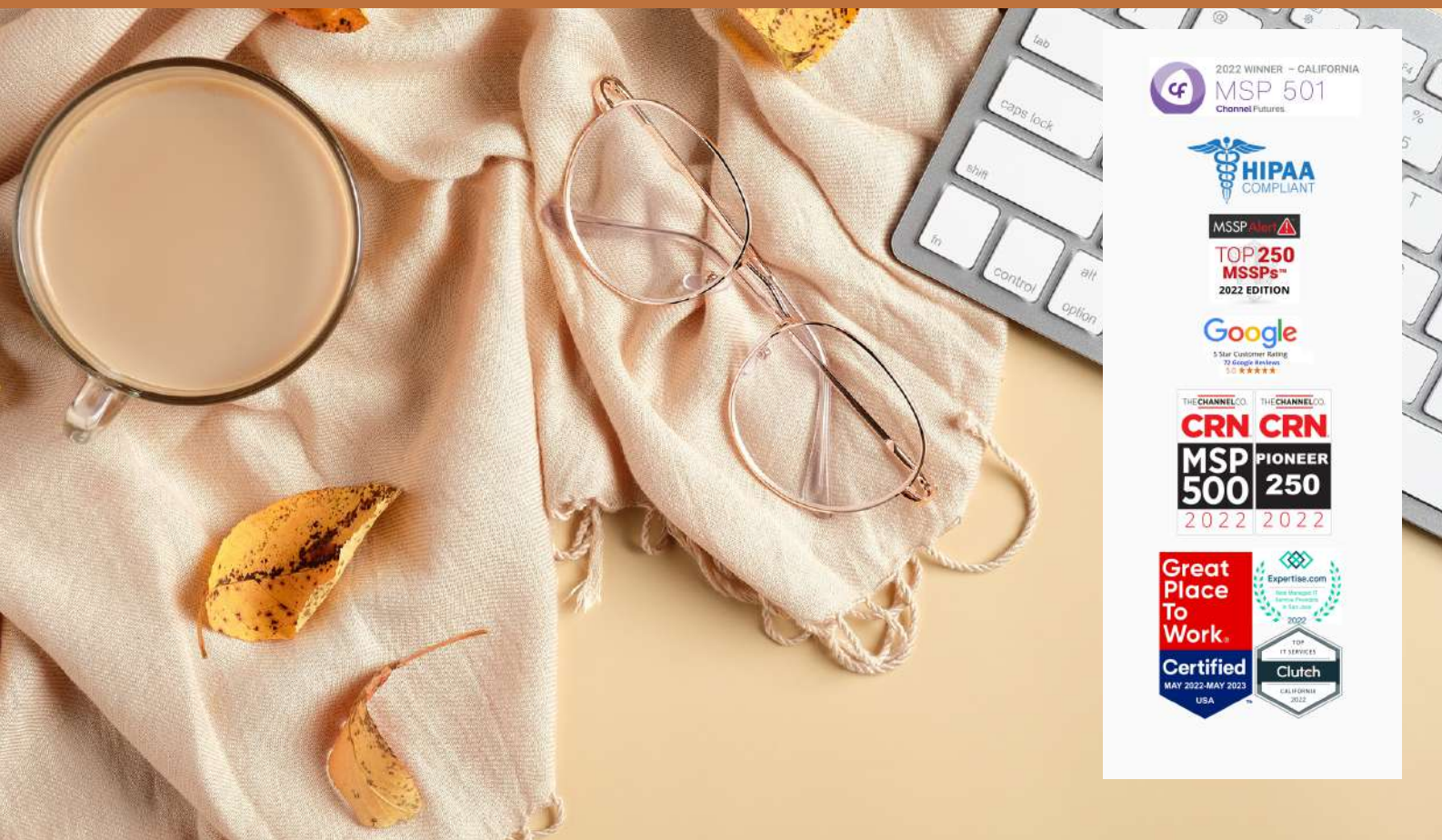


THE CHANGING OF SCAMS

How to avoid falling for new scams this season



2022 WINNER - CALIFORNIA
MSP 501
Channel Futures

HIPAA
COMPLIANT

MSSP Alert

TOP 250
MSSPs™
2022 EDITION

Google
5 Star Customer Rating
72 Google Reviews

THE CHANNEL CO. THE CHANNEL CO.
CRN CRN
MSP PIONEER
500 250
2022 2022

Great
Place
To
Work.
Certified
MAY 2022-MAY 2023
USA

Expertise.com
TOP IT SERVICES
2022
Clutch
CALIFORNIA
2022

THIS MONTH'S TOPICS:

Falling for Scams

New scams to avoid falling for...

School Scams

Internet safety tips...

Scam of the Month:

Give with caution...

Cyber Zen Den:

The importance of Mantras...

As technology continues to change like the seasons, so do scams.

Before enjoying all that the new technologies have to offer, it is important to know what scams to look out for, because while constant technological improvement can make life easier, it can also lead to many opportunities for cybercriminals, as well.

In this month's newsletter, take a look at some new scams to avoid falling for and how users of all ages can stay safe on the internet.

FALLING FOR SCAMS

NEW SCAMS TO AVOID THIS SEASON

September 17th was International Eat an Apple Day. Just like we can count on apples falling from the trees, we can count on cybercriminals creating new scams that users will fall for. Apples and scams have a few things in common. Each year more apples grow and new varieties are introduced. Similarly, scams are always growing and changing. Here are some new or modified scams to look out for this season.

1) **Mobile Payment Apps:** The convenience of mobile payment apps has changed the way we make purchases. Watch out for fake text messages from payment apps asking you to enter account information or click on a link. Don't send money to people you don't know, and if someone you do know requests money, always check with them first to make sure they have not been hacked.

2) **One-Time Password (OTP) Bots:** With the rise of multi-factor authentication, cybercriminals are finding new ways to hack accounts. Be cautious if you receive an OTP message out of the blue. The code might be sent by a legitimate company, but it was likely sent because someone else was trying to log-in to your account. The cybercriminal will then pretend to be with the legitimate company and call or text, asking you to provide the OTP sent to your phone. They will also try to ask you to enter the code if you did NOT authorize a change to your account. If you send the cybercriminal the code, they will be able to access your account.

3) **QR Code Scams:** As the popularity of QR codes continues to increase, cybercriminals are taking advantage. QR codes provide touchless options for payment, as well as access to restaurant menus, business cards, and more. Scammers are using QR codes to lead people to fake payment screens or infect their devices with malware. Avoid QR codes posted in public places such as parking meters or sent in unsolicited emails.





School Scams

Welcome Back Students!

Over the last few years, there has been a dramatic increase in technology used in the classroom. While this can provide a plethora of opportunities for educators and students, it also gives cybercriminals the chance to carry out many different types of scams. From shopping for new technology, to using it safely, there are many different ways everyone involved can stay cybersecure.

Buy Tech Supplies Safely

- Scammers can take advantage of supplies, like computer chips that are experiencing shortages, by posting fake in-stock listings.
- Be sure to shop through credible and well-known websites.
- Be wary of low prices and too-good-to-be-true offers.







Hiring a Tutor?

Tutoring can be very helpful for students starting challenging classes. Use referrals, check reviews, or go through a tutoring company to find a trustworthy tutor.

College Students

The "student-tax" scam involves a phone call to college students pretending to be from their university or government. The cybercriminal asks for money to pay for student taxes and tells the student they will not be able to take classes unless they pay.

Smartphone and Internet Privacy Tips

-  Install online protection software on phones as well as computers.
-  Use a lock screen. Only 56% of parents have a password on their phone. Only 42% put one on their child's phone, as well.
-  Be aware of apps and ads your child might see or have access to.
-  Free downloads of games or educational material from unfamiliar websites opens the risk of downloading a virus.



SCAM OF THE MONTH

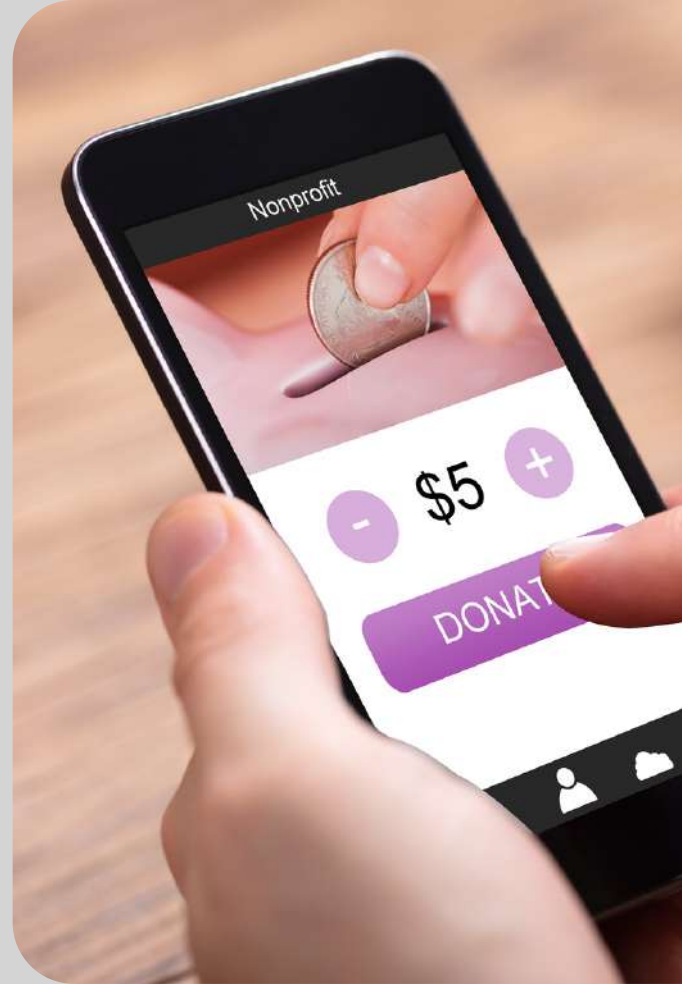
Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Hurricane season is in full swing and Samantha wants to donate to help the cities that have been hit the hardest.

Samantha planned on researching charities before donating, but when she saw a well-known news anchor post a link on social media to a charity collecting donations, she decided to donate through the link. She even reposted it to her own page so that others could easily donate, too.

A few hours later she saw another post by the news anchor. Her heart sank as she read his alert that the previous post asking for donations was a scam. A cybercriminal had hacked his account.

The link had seemed legitimate, but Samantha later realized it was a misspelled version of the real charity website. Frustrated and feeling naïve, Samantha did not donate again and did not alert her followers that the original post was a scam.



Did you spot the red flags?

- ▶ Samantha abandoned her strategy of research for what was convenient. Cybercriminals often use links sent right to a users' inbox or social media feed in order to catch them with their guards down.
- ▶ After clicking on the link, Samantha did not check the website name for spelling errors or check if the details matched with those of the real charity.
- ▶ Samantha reposted the link and did not take it down or alert her followers that it was a scam.



Charity scams often take advantage of disaster relief fundraising. Unsolicited messages or emails asking for donations after hurricanes, earthquakes, or wildfires should be treated with caution. Always research and look at reviews before donating.



For those affected directly by a storm, use references and research before hiring someone to repair the damage. Ask anyone you hire for a written contract and read it carefully. Do not to pay in full before the work is done, especially if the payment method is cash.



September often brings disasters such as hurricanes or other storms. Cybercriminals often take advantage of those who generously try to help. By researching, looking at charity ratings, and staying educated on the tactics used by scammers, it is still possible to give safely to trustworthy charities who truly do make a difference for those in need.

Key Takeaways

Cybercriminals often take advantage of new technology and seasonal trends. Being aware of how these latest trends can be used by cybercriminals will allow for a better and safer experience with technology, overall.



Be intentional when using new technology: While new technology can be exciting and convenient, remember scammers will find ways to take advantage of the technology too.



Research, referrals, reviews: These 3 R's are a great way to remember what to do before purchasing an item or service. Referrals from people you know are a great place to start. If you do buy online, research and read reviews of the company.



Always be skeptical of unsolicited messages: If someone you don't know contacts you first, enter the conversation with a healthy amount of skepticism.

Mantra

A word or saying that is repeated during meditation or yoga practice. A mantra is used to quiet the mind, create calm, and to help with concentration.

How does this relate to cybersecurity?

While it is beneficial to educate ourselves on all of the scams and tactics of cybercriminals, it can be overwhelming. Taking a second to create calm can make staying cyber secure seem much less daunting.

Now apply this concept to cyber-awareness.

Be mindful and focused as you browse the web. Concentration and intentionality can make all the difference in spotting a phishing message or scam.