Issue 1 | Volume 10 | March 2024

ADDRESSING THE NEEDS AND SECURING THE FUTURE

Helping secure your world

Security Solutions

Editor's Note:

Greetings,

As we navigate the digital age, it becomes increasingly imperative to equip ourselves with the knowledge and strategies necessary to safeguard our security and privacy. In this March 2024 edition of our Security Solutions Newsletter, we address a spectrum of threats and provide actionable insights to fortify our defenses.

"8 Smart Easy Ways to Travel for Less" introduces practical tips to ensure that your adventures remain not only enriching but also financially prudent, guarding against potential travel-related pitfalls.

In "CEO Swindle," we expose the intricate schemes employed by cybercriminals to impersonate executives, emphasizing the importance of vigilance and robust authentication measures to thwart such fraudulent activities.

"Don't Be the Loser in These 7 Online Games Scam Tricks" serves as a comprehensive guide to recognize and combat deceptive practices within the gaming community, empowering readers to enjoy their online experiences safely and securely.

Lastly, "How Your Face Could Launch Identity Theft" probes into the intersection of facial recognition technology and identity theft, urging caution and awareness in the face of evolving privacy concerns.

As you delve into these articles, I encourage you to remain proactive in implementing the recommended measures and to share this knowledge with your peers. Together, we can foster a safer digital environment for all.

Stay vigilant, stay informed, and stay secure.

At Amalgamated Security Services Limited we will continue to fulfill our commitment to provide quality service for all customers and in keeping with this commitment we do hope you find these articles and the safety techniques helpful.

Best regards,

Carril Reyes-Telesford
Regional Marketing Specialist

8 Smart, Easy Ways to Travel for Less in 2024

You're not imagining it—trip costs are pricier than they've been in five years. We've got some simple ways to keep costs down even while rates are headed up. Don't book your vacation until you read this

Travel is so expensive post-pandemic. But I don't want to give up the idea of an annual vacation. How can I keep costs down? —Tripping Out Over Expenses.

Experts predict that this year will be the busiest ever for travel since before the pandemic. And for many, it's already feeling like it might be the priciest. According to NerdWallet's February 2024 travel inflation report, the cost of hotels, entertainment, and dining out are rising, with overall travel expenses for the past 12 months up 3.1 percent through January 2024 compared to pre-pandemic levels.

Hotels will be a big vacation investment. Lodging rates increased 5.2 percent between December 2023 and January 2024 alone. And traveler beware: the average daily hotel rate is projected to grow nearly 5 percent more in the next year, according to hotel-commerce platform SiteMinder. There's been little respite from room rates hovering near all-time highs at properties across the U.S. this winter, and staff shortages will likely mean continued high prices but fewer services. You're getting gauged even more for dining out: in January, prices for restaurant meals were 25.6 percent higher than the same month four years ago.

There is some good news: airfare—on domestic routes in particular—is predicted to drop 16 percent this year, according to Kayak. The travel-research engine estimates it will cost $461 on average to fly in the U.S. I recently booked a round-trip, direct flight from Denver to Newark, New Jersey, in April on United for a very reasonable $227. That's about half of what I was paying for the same flight in April 2018.

That said, the overseas flights I've booked for spring and summer travel have given me serious sticker shock. International airfare departing from the U.S. is up 10 percent compared with 2023, according to Kayak. In the past, I've scored direct flights from Denver to Los Cabos, Mexico, for under $400; a flight for late March this year was $1,200. Similarly, a late-May flight from Denver to Majorca, Spain, was priced at over $3,000, when in the past I've seen it for as low as $600.

Some experts are optimistic that additional flights and routes, especially those from upstart low-cost carriers like Breeze Airways and Norse Atlantic Airways, will help lower international fares, but I'll believe it when I see it. For now your best strategy is to book overseas fares early. According to Kayak, eight months is the sweet spot and can save you between 8 and 18 percent.

If you're on a budget but still want to go big in some fashion, don't despair; you can still have an affordable annual vacation if you're willing to be flexible on timing, strategic about choosing a destination, and plan ahead. Here are some of my tricks, plus tips from industry experts on how to make that happen.

1. Travel in the Shoulder Season

A waterfall surrounded by lush green trees and plants is a hiker's dream in Costa Rica.

The shoulder season in Costa Rica can be wet, depending on where you are, but the effects are emerald tropical forests and fully flowing waterfalls like 230-foot-high La Fortuna.

Shoulder seasons are periods when destinations see fewer tourists but aren't closed for the off-season. The perks are fewer crowds and often great deals on hotels and flights, but on the flip side, shops and restaurants may be shuttered or have

limited hours. Weather can also be a gamble. In Mexico, for example, September and October are the slowest months of the year for tourism; they're also the wettest, and the time tropical storms are most likely to hit both coasts, says Zach Rabinor, founder of Journey Mexico.

Don't dismiss destinations during a rainy season, though. In Costa Rica, you can save 30 to 40 percent between August and November and enjoy deserted beaches and lush rainforests, says Javier Echecobar, cofounder of Journey Costa Rica. "Those months are considered rainy, but usually with clear mornings followed by afternoon showers," he says, adding that on the Caribbean side of the country, the coast tends to be very clear during those months, a result of microclimates.

If you're seeking value above all else, you may need to skip bucket-list destinations this year, even during the slow seasons. I booked a trip to Rome in March, and while streets and major attractions were quieter, prices weren't cheaper for my flight, hotels, or restaurant meals.

Jenna Swanna, a travel agent with Embark Beyond, says you'll find more value visiting less iconic cities during shoulder season. "A room in Paris could easily cost two or three times the amount of a room in Madrid," she told me.

2. Pay Attention to the Extra Costs of Travel

I used to be quick to jump on a cheap airfare or hotel rate without considering the bigger picture. When choosing between a 6 A.M. flight priced at $450 versus a 10 A.M. priced at $500, I'd book the seemingly more affordable option. What I didn't factor in was that getting to the airport would tack on extra fees: the $10 bus route I typically take doesn't run that early, which meant I'd have to pay upward of $100 for an Uber, or drive and fork over as much as $50 a day for airport parking.

Additionally, major airlines are piling on more fees, for everything from checked bags to select seats, and airline websites often use design strategies known as dark patterns used to push consumers to buy extras (like a rental car or trip insurance) during their purchase.

3. Book an All-Inclusive Vacation

A family of four on a catamaran cruises away from the Caribbean shoreline of Mexico and into deeper turquoise waters.

Imagine having this excursion included in the price of your vacation instead of shelling out additional cash through an independent outfitter. Club Med's Cancun resort is one of its most popular beachfront properties.

Once associated with budget travelers and bottomless drinks, the all-inclusive-resort model has gone upscale, with properties that feature Michelin-star restaurants, fine wines, and privately guided activities. The initial price tag can seem spendy, but when you factor in everything, you get incredible value.

And all-inclusive stays aren't just for beach holidays. Package-vacation pioneer Club Med now offers properties in Quebec and the Alps. A family of four booking Club Med's five-night ski getaway in Charlevoix, Canada, can save upward of $7,000 compared to a plan-it-yourself ski vacation in Aspen, Colorado—even after factoring in airfare.

At the four-season Club Med Quebec Charlevoix, guided hikes and wellness experiences are offered year-round. In winter, lift tickets and dogsledding are just two activities guest can enjoy.

4. Use a Travel Agent

As a seasoned traveler, I used to think a travel agent would be of no use for me. I now view these professionals as travel wizards. They have industry connections that translate to free room

upgrades and special perks, like resort credits, complimentary breakfast, and occasionally other amenities such as a bottle of wine waiting in the room, free airport transfers, and VIP access to museums and adventure sites. If anything goes wrong, they're on call to help. And they know how to score great deals. When I reached out to a travel agent about the exorbitant Majorca flight, he was able to bring the cost down to $1,753—almost half of what I was looking at spending—by mixing airlines and connections.

The Balearic island of Majorca, Spain, beckons with swimming in protected coves, mountain trekking, and deep-water-solo climbing. Getting to this adventure oasis, however, can prove to be pricey, especially in the high summer season.

5. Check the Exchange Rate—and Head to Where It's Most Beneficial

Last summer I traveled to Croatia, not realizing the country had embraced the euro. When I visited in 2020, the dollar's strength against the kuna made Croatia feel like an economic destination. But now it's just as pricey as vacationing in France or Italy.

A good exchange rate gives you extra buying power to maximize your travel experience (think: more activities and spectacular meals). In Canada, given the strength of the U.S. dollar, everything is essentially 30 percent off for Americans; in Australia, around 35 percent. Asian countries such as Vietnam and Indonesia, and South America nations like Colombia and Argentina, are also excellent places to stretch your dollar.

6. Let New Flight Routes Dictate Your Destination

Low-cost carriers offer some of their lowest prices when launching new routes. Frontier, for example, has promoted fares as low as $19 in the days following the announcement of new routes. And even after promotional fares disappear, having a new airline on a route adds competition that tends to nudge prices down. Many major airlines are also launching new routes this year. American, for example, will begin flying to the new airport in Tulum, Mexico, this month. Follow travel sites like Skift and the Points Guy, which keep up with this information.

7. Reconsider Hostels. Many Are New and Hip.

Yes, the grungy backpacker hotels of your post-college days still exist, but there's also a crop of clean, budget-friendly hostel chains attracting crowds. Check out A&O, Freehand (which describes itself as "a collection of hotels that combine the social culture of a hostel"), and Generator. According to Oliver Winter, founder of A&O, the largest hostel brand in Europe, nearly 28 percent of guests are between the ages of 25 and 34. Boutique hostels often offer private rooms with an en suite bathroom, bunk rooms to accommodate families or groups of friends, and a place to make meals so you're not forced to fritter away your budget dining out. I've stayed in a four-bed bungalow bunk room at the Freehand Miami with friends, and it felt as stylish and immaculate as a boutique hotel, plus, the bar, Broken Shaker, makes some of the best drinks in the city.

8. Save on Meals (but Still Eat Your Heart Out)

I always try to book a hotel room that includes breakfast in the rate. My strategy: eat a hearty, late breakfast and then pocket a muffin and a banana for a snack later on that can tide me over until an early dinner.

Taking advantage of local street-food scenes can also save you heaps. A&O's Winter says that Florence, Italy, is a little-known street-food city (though not full of food trucks, as Americans might imagine, but shops that sell various hot and cold sandwiches and beverages you can enjoy on the street). He likes Da' Vinattieri, close to the National Museum of Bargello.

Reprinted from Outsideonline.com

CEO Swindle

A manufacturing firm transfers thousands to scam artists after falling victim to CEO fraud.

Social engineering involves the use of deception to manipulate individuals into carrying out a particular act, such as transferring money, handing over confidential information, or clicking on a malicious link, and it's causing serious financial harm to businesses around the world.

One of the most common types of social engineering is CEO fraud.

This is typically a targeted attack where a fraudster impersonates the CEO or another senior executive within the organization and instructs a member of the finance department to make an urgent payment to a particular account for a specific reason.

More often than not, the CEO or senior executive in question will have had their email account compromised. But you don't even need to be hacked in order for this kind *of* fraud to be carried out. Some fraudsters will go off publicly available information such as email addresses.

Any business that transfers funds electronically can be susceptible to losses of this nature.

Phishing

One of our policyholders affected by a case of CEO fraud was a manufacturing company, specializing in the production of machinery used in the textile industry.

The scam all began when the CEO fell for a credential phishing email.

Credential phishing emails are used by malicious actors to try and trick individuals into voluntarily handing over their login details. Typically by directing them to a link that takes them through to a fake login page.

In this case the CEO received an email *from* what he thought was Microsoft. The email stated that his account details needed to be validated in order for him to continue to use the Outlook service without disruption. As the email appeared to have come from an official source, the CEO clicked on the link. The link took him through to a seemingly legitimate landing page, where he inputted his email login details. Assuming that his account had been validated, the CEO gave no further thought to the incident.

However, by inputting his credentials on this login page, he had actually passed on his details to a fraudster who could now access his account.

Gaining access to the CEO's email account allowed the fraudster to gather valuable information about how invoice payments were processed at this company. For example, it allowed the fraudster to take a look at previous Invoices that had been sent from the insured's contract manufacturers and suppliers and to identify the main Individual in the insured's finance department responsible for paying invoices and authorizing wire transfer requests.

What's more, it also allowed the fraudster to gain access to the CEO's Outlook calendar and establish what the CEO would be doing on any given work day.

Having worked out the CEO's schedule from his calendar, the fraudster waited until the CEO was travelling abroad for a few weeks on a business trip. With the CEO out of the office and with the chances of the scam being uncovered much reduced; the fraudster chose his moment to strike.

The fraudster's plan involved posing as a member of the accounts department for one of the insured's contract manufacturers.

The fraudster's first step was to set up forwarding rules in the CEO's email account.

Forwarding rules are settings that can be applied to an email account which ensure that emails that fall within a certain criteria are automatically forwarded to a specific folder or to another email account.

In this case, the fraudster set up two rules to ensure that the CEO didn't come across any of the emails related to the scam whilst he was away on business.

The first rule that was created meant that any emails from the individual responsible for approving payments were immediately marked as read and sent directly into the account's deleted items folder.

The second rule meant that any email that included a keyword such as "invoice" or words used on this particular contract manufacturer's trading name, in the subject line was marked as read and automatically sent to the deleted items folder.

With the background work now done, the fraudster sent an email to the CEO purporting to be from the accounts department of the contract manufacturer, attaching an invoice *for* $47,500 and explaining that there had been a change of account details. To add an aura of authenticity to the scam, the fraudster used one *of* the actual contract manufacturer's invoices as a template.
So to all intents and purposes the invoice looked normal, it featured the contract manufacturer's logo and address on the heading of the invoice

and carried a breakdown of the work carried out. The only difference was that the account details had been altered by the fraudster.

As a result of the forwarding rules in place, this email was immediately marked as read and sent to the deleted items folder. The fraudster then logged into the CEO's account and, posing as the CEO, forwarded this email to the individual within the finance department responsible for authorizing payments and requested that the payment be made that day. As the CEO was out of the office and because the email requesting that the invoice be paid had come from his account, the employee in the finance department assumed that this was a legitimate request and duly paid the invoice.

Having seen that the ruse had worked, the fraudster decided to try their luck and now sent through another invoice a few days later.

On this occasion, due to the fact that it had only been a few days since the last invoice had been paid the employee in the finance department responded to the CEO about the request to check that this was correct. Because of the forwarding rules put in place, however, the CEO was oblivious to the employee's response- only the fraudster was aware of it. In the guise of the CEO, the fraudster responded and explained that all was in order and that the invoice should be paid.

With the employee in the finance department genuinely believing that they were in correspondence with the CEO and with any objections and queries about the payments being swiftly answered, the fraudster managed to get two further invoices approved, bringing the total amount paid out to $190,000.

It was only upon the CEO's return to the office that the payments came up in discussion and the scam was uncovered. Our policyholder reported the incident to local law enforcement and attempted to recover the funds from the recipient bank.

But all of the money had been moved out of the fraudulent account and the prospects of a successful recovery were deemed to be remote. Thankfully for the insured however they had purchased cybercrime cover on their cyber policy with CFC and were able to recover the loss in full.

This claim highlights a few key points. Firstly, **it illustrates how CEOs and senior executives are prime targets for cybercriminals.** CEOs and senior executives usually act as the face of their respective companies and as a result they tend to have bigger profiles on company websites and social media accounts, allowing cybercriminals to gather valuable information about them.

In addition cybercriminals know that employees are instinctively less likely to question and more likely to act upon instructions from senior executives. CEOs and senior executives therefore need to be especially conscious of sticking to good cyber security practices, and **employees need to be particularly alert to suspicious emails from senior executives** and have robust call-back and authentication procedures in place.

Secondly, it shows that cybercriminals are becoming much more sophisticated. In the past. It was not uncommon to see blatant attempts at funds transfer fraud over email, with an urgent appeal for help or bogus prize giveaways being just two examples.

Now, however, we are seeing far more nuanced attacks. In this case the fraudster managed to trick the CEO into volunteering his email login details, identify who was responsible for authorizing payments and work out when the CEO was out of the office on a business trip, as well as setting up forwarding rules in the CEO's in box to avoid detection and making use of one of the Insured's genuine contract manufacturer's invoice templates to add authenticity to the scam.

Finally, this claim also discredits one of the most common objections that organizations have to purchasing cyber insurance: namely that by investing heavily in IT security, they have no need for cyber insurance. The fact IS that the vast majority of cyber incidents are a result of human error. With increasingly sophisticated attacks like this on the rise, it makes it very difficult for employees to tell the difference between a real email and a fake email or a real invoice and a fake invoice. Furthermore, with more and more financial transactions being carried out electronically, the number of opportunities for cybercriminals to steal these funds has never been greater.

Having good training and authentication procedures in place can certainly help reduce the risk of an event like this happening, but it's impossible for any business to be completely impervious to these kinds of attacks. This is why cyber insurance should be a part of any prudent organization's risk management program; acting as a valuable safety net should the worst happen.

Case Study performed by CFC

DON'T BE THE LOSER IN THESE 7 ONLINE GAMES SCAM TRICKS

In a business said to be worth a total of more than $15 billion, online games scam incidents have soared in the past couple of years.

Fans of multi-player role-playing games, cell phone quizzes and online casinos have handed over all kinds of swag, from virtual "gold" and other imaginary credits, through real cash to personal details in a phishing scheme aimed at identity theft.

The irony is that, in at least some online games, it's perfectly legit to scam others within the scope of the gameplay, though not, of course, in the real world!

Here are the seven most common types of Internet scams:

1. THE GATEWAY TO TROUBLE

Scammers trick victims into paying a one-off fee, usually about $40, for supposedly unlimited downloads of games for PCs and gaming devices like PSPs and Xbox. All you actually get for your money is a set of links to file sharing sites whose legality is, at best, dubious. These "torrent" sites enable users to swap games and other files -- in most cases, it's a form of piracy. We don't recommend ever using these file sharing sites because they not only peddle this copied, pirated software but also host a minefield of malware you can easily and unknowingly download. Even so, access to these sites does not require a $40 passage through a gateway to find them!

2. ONLINE CASINO SCAMS

Americans spend a small fortune every month playing online games like poker, blackjack, roulette and other casino games. There are no federal laws against this (though it's illegal in some states) but banks and credit card companies are effectively prevented from transferring money directly to online gaming sites and many states forbid the operation of gaming sites based within their jurisdiction. This often means players have to channel their money through third-party operators and play on casino sites based outside of the US -- two highly risky activities. Some of these operations are perfectly honest and reliable. But others are no more than fronts for stealing your cash or confidential information. They use all kinds of deals to entice you, including free bonus plays (once you've deposited a certain amount) and good winning odds (usually fabricated).

Action: Do an Internet search on any site you're thinking of using -- but beware, some phony sites actually have other sites carrying bogus recommendations for them or even dressed up as anti-scam web pages. Even with legitimate operations, check the fine print -- the terms and conditions -- carefully. Some conceal limits on winnings.

3. PHISHING VIA AN ONLINE GAMES SCAM

This is no more than a gaming version of the well-known phishing scheme in which a user is fooled into giving away his/her account details. Players receive an email asking them to confirm a password change. The link in the message takes them to a phony sign-on page (notably for the hugely popular game World of Warcraft) that requests their "old" sign-on details. Once they have this, the scammers immediately log on to the victim's account, download their credits or virtual gold, which they then sell online.

Action: You'd think WoW gamers would be savvy enough not to fall for this, but they do. The answer, of course, is not to click on links in these messages but to go directly to the site

admin and check your details there.

4. SALE OF VIRTUAL ASSETS

Because many online games use credits or other assets that have a nominal monetary value, players sometimes trade these, even though some sites, like eBay, have tried to stamp out the practice, mainly because so many of these assets are stolen. On top of that, crooks also offer for sale credits and virtual assets that they don't even own.

Action: No matter how tempting, just don't trade this way. You'll likely get your fingers burned.

5. GET PAID TO TEST VIDEO AND ONLINE GAMES -- NOT

Again, this is a variation of a well known scam -- phony work from home jobs. In this con, scammers tell victims they can earn up to $100 an hour testing beta versions of online games and other video entertainment -- plus they get to keep the software.

Action: Unless the job is with an established developer, and usually they don't pay, this likely is a scam in which you'll be asked to pay for a list of leads or a useless training kit that supposedly will earn you reviewer credentials.

6. CELL PHONE DIALERS

In this online games scam, users download a game onto their cell phones that secretly dials long distance and premium line calls -- in one reported case apparently dialing a number listed in the Antarctic! Users don't know what happened until their phone bill arrives -- and even then only if they bother to check the call logs in detail.

Action: This scam principally targets users of Windows Mobile phones and the particular program in question features an anti-terrorism game. But the general rules here are to be cautious about downloading free phone games and always to check your bill carefully (and frequently, you can usually do this online).

7. MORE CELL PHONE TRICKERY

Another cunning online games scam that exploits cell phone users uses social networking games that require players to earn credits so they can run virtual businesses and other activities.

More Scam Reports: How to Find Out if Your Social Security Number has Been Stolen, Internet Dating Scams and Phishing by Phone

Desperate for these credits, victims encounter other "players" or even receive emails, offering them free credits if they'll view ads or take part in other quizzes.

Sometimes, the advertising-driven offers are genuine but the quizzes -- frequently of the "test your IQ" variety -- ask users for their cell phone numbers so that their results can supposedly be texted to them.

Hidden in the fine print for these offers is the old familiar trick of signing victims up for a recurring monthly fee (charged to their cell phone and usually about $10) for services like ring tone downloads, astrology forecasts, and so on. This online scam allows crooks to target youngsters who might not have access to credit cards but whose cell phone bills are often paid by their parents.

Action: Make sure your kids are aware of this scam, always read the fine print and, again, carefully scan your monthly phone bill.

Reprinted from Scambusters.

HOW YOUR FACE COULD LAUNCH IDENTITY THEFT

You probably don't think of your face as a collection of data when your peer at it in the mirror or a photo. But it is.

Cameras may record your facial image, but software can convert it into a stream of digits - representing biometric patterns - that can and is being used for security. And now scammers have joined the fray.

We already know how scammers use stolen photos in romance scams. But now evidence is starting to emerge about mobile apps that can use facial data to drain a bank account. It's already appearing in parts of Asia. And you can expect to see it on our shores in the not-too-distant future.

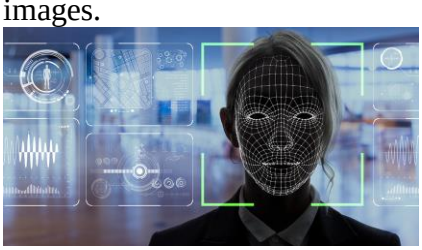
WHAT IS FACIAL RECOGNITION?

We humans recognize each other using memory banks in our brains. Facial recognition software does the same, comparing what it sees with existing records.

It's one of the key biometric processes we wrote about in issue #866: How Safe Are Fingerprint and Facial Recognition Sign-ons? And it helps organizations and security services confirm we are who we say we are. At least that's the theory. But it doesn't take much of a leap of imagination to see its potential for a scam. If someone can fake your face, they can pretend to be you. And that's exactly what's happening.

FACIAL RECOGNITION SCAMS ARE REAL

A new report from Singapore-based cyber security firm Group-IB claims that malware that finds its way onto some mobile phones can steal facial data. It uses artificial intelligence (AI), the same that's used for creating deepfake images.



Victims are tricked into providing a face video and a copy of their ID card supposedly for a new security app. The image and info are then used to open or access victims' bank accounts. We won't explain how it's done but if you're interested you can read the full, widely-reported Group-IB research: Face Off: Group-IB Identifies First iOS Trojan Stealing Facial Recognition Data.

The real worry about this latest scam is that the perps found a way of getting their malware onto iPhones. Initially, this was through Apple's app-testing program Test Flight. When Apple put a stop to that, the crooks, believed to be based in China, found a workaround via mobile device management (MDM) software usually only used by IT managers to control employee iPhone usage.

This is another frightening example of how identity theft is exploiting new technology.

Cybercrooks may intercept facial recognition data when it's being sent over the internet. Or they might steal it during data breaches. And in Latin America, con artists are employing what's been called the "false face scam."

According to cybersecurity specialists Insside, the fraudsters use mannequins and photos of their victims to open bank accounts by fooling the verification process.

"Acquiring a user image is easier than you might think: simply obtain images of personal documents or search for photos online, print them life-size, and then attach them to a mannequin to use for facial verification during account opening," the firm explains.

CAN YOU PROTECT YOURSELF AGAINST FACE RECOGNITION SCAMS?

As we noted, facial recognition scams are currently active outside of the US. But, as a report on the tech consumer website Tom's Guide noted

recently: "As with other malware campaigns, if this one proves successful, the cybercriminals behind it could expand their operations to target both iPhone and Android users in the US, Canada, and other English-speaking countries."

So, can your protect yourself against this risk?

If you use an Android phone, you should definitely have high-level security software installed and avoid downloading apps from anywhere but Google Play Store.

For iPhone users, Tom's Guide says don't install any apps through TestFlight.

"The same goes for adding a MDM profile to your iPhone," says the site. "Your employer is the only one that should be asking you to do this and that's only if you have a company-issued iPhone."

Beyond these specific actions, the emergence of facial recognition scams highlights the need to restrict the availability of your face images on the likes of social media sites.

Beware also of any app that asks you to scan your face. You need to be sure the app is legit and so is its need to have a picture of your face.

Finally, as always, you should regularly and frequently monitor your financial accounts and credit records for signs of activity you didn't initiate. Take immediate action to notify the relevant organization as well as law enforcement.