I'M AN AVID MOVIE STREAMER,

and it's not unusual for me to receive emails from Netflix about things to watch. So a new message about updating my account information didn't seem out of place—especially as it featured the familiar red Netflix logo. Here's what the email looked like:

We were unable to validate your billing information for the next billing cycle of your subscription. therefore we'll suspend your membership if we do not receive a response from you within 48 hours.

Obviously we'd love to have you back, simply click restart your membership to update your details and continue to enjoy all the best TV shows & movies without interruption.

We're here to help if you need it. Visit the Help Centre for more info.

-The Netflix Team

This common 'phishing' scam was engineered to trick the recipient into providing their credit- or debit-card number, bank account details or Netflix password. Through email (often with questionable grammar, as with the message I got), text messages, social media requests or old-fashioned phone calls, cybercriminals are doing everything in their power to deceive and defraud you. All around the world, people are falling victim to data breaches and viruses, as well as ransomware (when you're locked out of your computer unless you pay to regain access).

Cybercriminals are often linked to attacks from China and Russia (often state sponsored), India (where many call centres are located) and parts of Africa (Nigerian prince, anyone?). That's because it can be difficult to find and charge perpetrators in those places. But the attacks can come from anywhere.

Cybersecurity experts at Symantec say the United States experiences the most cybercrime. In 2021, it cost Americans older than 50 nearly US$3 billion, a 62 per cent increase from the prior year, according to the FBI's Internet Crime Complaint Center. In fact, the number of victims could be much higher, in part because many are seniors who may not know how to report it, or even that they have been scammed at all.

In Canada, about C$379 million was lost to scams and fraud in 2021 for all age groups, an increase of 130 per cent compared to the year prior, according to the Canadian Anti-Fraud Centre (CAFC). The UK has been hit hard, too, with more than £1.3 billion gained by cyber-scammers in 2021, says UK Finance, which represents the banking and finance industry there. About 40 per cent of this amount was obtained by fraudsters convincing people to pay into a bank account.

Cybercrime is rising fast in India too: From over 9,600 crimes in 2014, the country saw 1.6 million cybercrimes being reported between January 2020 and December 2022, the Union Minister of State for Home Nityanand Rai told the Indian Parliament in December last year. India sees 3,500 online financial frauds every day, according to India's national cyber-security coordinator Dr Rajesh Pant.

The FBI, in its Internet Crime Report 2021, said India had recorded the fourth-highest number of cybercrime incidents in the year, preceded only by the US, the UK and Canada.

CYBERCRIME IS RISING FAST IN INDIA: REPORTED CASES WENT FROM 9,600 IN 2014 TO 1.6 MILLION BETWEEN 2020 AND 2022.

These crimes are pervading all aspects of daily lives of Indians—paying off utility bills, answering a video call from an unknown caller, ordering food online, looking for a job, or even booking a hospital appointment, could land you in the throes of a cybercrime.

Driving this rise is a dangerous mix of an aggressive push towards using digital technologies combined with poor digital literacy, said Ritesh Bhatia, a seasoned Mumbai-based cybercrime investigator. "There is a tremendous digital push in India," said Bhatia, referring to a push by both, businesses to adopt digital tools as well as by the Indian government as part of its 'Digital India' programme. "But we are not a country with high levels of literacy about, both, digital technologies as well as the English language. Often, the language employed in these fraudulent emails and messages can be difficult to comprehend," said Bhatia.

The problem is getting worse. According to Cybersecurity Ventures, a New York-based publication, global cybercrime is expected to balloon to US$10.5 trillion annually by 2025, up from $3 trillion in 2015. If it were measured as a country, cybercrime would be the world's third-largest economy, after the United States and China and ahead of Japan, Germany, the UK, India, France, Italy and Canada.

Reasons are varied, but many cybersecurity experts cite the pandemic as a catalyst, when much of the world was forced to work from home, often without the same security protocols as they have at the office. This made it more likely that computer viruses would be let in, says Vishnu Varadaraj, a senior director at software-security company McAfee Canada. The number of ways they could take advantage of us increased, he says, especially as we're using more devices to access online accounts for things like banking, shopping and social media apps.

THE MOST COMMON THREATS

Here are some of the widespread cybercrimes happening right now.

PHISHING AND SMISHING

No respectable company or government department will email to ask you to confirm your identity by filling out forms. These authentic-looking emails are often referred to as 'phishing'—luring you to a phony website to input information. (When these come via text message, experts refer to it as 'smishing,' for 'SMS phishing.')

An email could have a logo like that of your bank or credit-card company. The message says that someone is trying to access your account, and that you need to log in immediately and change your password. But, unknown to you, the link you click takes you to a fake website, and your current password and private financial information go to the fraudsters. Money can now be withdrawn from your account or applied to your credit card. You may then be locked out because the criminals may have changed your password.

Electronic forms of payment like cryptocurrency, gift-card codes and money orders are popular among cybercriminals because they require no in-person interaction, are difficult to trace back to the fraudster and can be accessed from around the world.

Never click on links or attachments in an email asking you to confirm your

details. When in doubt, contact the company or organization to ask if it was really them. Use a phone number that you look up yourself; do not use any number provided in a voicemail or call.

'VISHING'

Don't trust anyone phoning to tell you they're from the tax department, a bank, your internet service provider or a 'tech support' department. Even if you recognize the number, these things can be easily spoofed.

"This 'voice phishing,' or 'vishing,' scam can be very convincing and

SCAMMING INDIA

The Sex-tortion Scam:
In January, 71-year-old Mumbai businessman Rajesh Deshpande was in his workshop one afternoon when his phone rang. It was a video call from an unknown number. During my interview with him, he recalled, how, when he answered the call, he saw a young woman, who looked to be in her late 20s. He asked her who she was, but she did not respond. Instead, she began undressing. Shocked, Deshpande froze. Then he called out to her in alarm, asking her what she was doing, but still no response. It was just a few seconds and then he disconnected the line.

Before he could process what had happened, his phone rang again, this time, an audio call from another unknown number. On the other end of the line was a man who said he had a video that showed Deshpande indulging in online sex with a young woman. He would upload the video on the internet and send it to Deshpande's Facebook friends list if Deshpande did not pay ₹50,000 immediately. Deshpande was stunned. He immediately took the SIM card out of his phone, shut it down, deleted his Facebook profile and got a new number, hoping that they don't reach him again.

Deshpande was lucky, but many others weren't. In the same month, a 68-year-old businessman in Ahmedabad ended up paying ₹2.7 crore to sextortionists; another retired bank employee lost ₹17.8 lakh to the same scam. Bhatia, the cybersecurity expert, said this was "the most common scam" and one that is occuring with alarming frequency in India.

The Alcohol Ordering Scam: A woman in Mumbai was duped of ₹5.35 lakh; a senior citizen in Pune saw over ₹3.16 lakh from his savings siphoned off; a Gurugram man lost nearly ₹2 lakh, a Bengaluru woman lost ₹1.6 lakh; another SEBI official in Mumbai was swindled of over ₹1.6 lakh. All of them, across the country, had a common link—they were scammed while trying to buy alcohol over the phone, purportedly from a neighbourhood wine shop.

The scam has a simple modus operandi: manipulating the online contact details of wine shops, re-directing customers to fraudulent numbers and then tricking them into sharing bank details under the pretext of paying for alcohol that never gets delivered. A news report in October 2022 counted over 50 people to have been targeted in Bengaluru and Hyderabad alone. In September 2019, I nearly fell victim to this myself. Looking for a few beers, I found the number of a local wine shop on Google and called them up. The man on the line promised to deliver the beers, but demanded money beforehand. He would take neither cash on delivery, nor bank transfers—only through a link they would share with me. When I refused, he turned angry. When I called him out, he became abusive. I realized then that I had just saved myself from turning into a statistic.

Continued on page 51

threatening," warns Theresa Payton, a renowned cybersecurity expert who served as the first female White House chief information officer from 2006 to 2008. Based in Charlotte, North Carolina, Payton is the CEO and founder of Fortalice Solutions LLC, a cybersecurity and business-intelligence operations company, and is the author of several books on cybersecurity.

A popular phone scam goes something like this: "I'm calling from Microsoft. We've had a report from your internet service provider of serious virus problems on your computer. Can I help?" They'll tell you the problem means you could be without internet access if the issue isn't resolved.

They may give you instructions for granting them access to your computer from wherever they are—and they take control over your mouse and keyboard as if they were sitting in front of it. The fraudster then collects your data, either immediately or by installing hidden software that can send them information.

Seniors are often, but not always, the victims, though more members of Generation Z (born after 1997) are falling for vishing and online scams. In the US alone, phone-related scams cost Americans a staggering US$39.5 billion between March 2021 and March 2022 according to Truecaller, an app that identifies and blocks spam calls and texts. This was the highest amount recorded since this annual report, done in partnership with The Harris Poll, began in 2014.

Fraudsters may claim they're with the Internal Revenue Service (IRS), says Payton, using fake names and I.D. badge numbers, and may demand you pay fake tax bills immediately or else face arrest or other legal action.

"If you have caller ID, it may even look like it's from a bank or the IRS, as I recently experienced," Payton adds. "So just know that there are certain things your bank or the government will never do—and that's call, email or text you and tell you that you're going to be fined or arrested if you don't do this or that."

RANSOM EMAILS

Another scenario is when your passwords are held for ransom if you don't pay up. This kind of extortion message was received by Bob Lotich, a Franklin, Tennessee, educator and personal-finance expert. "The password that I had used on hundreds of sites was sitting there right in the subject line," Lotich wrote on his blog. "The email explained that they not only had my password but had hacked into my webcam."

The cybercriminals informed him that if he didn't send US$2,900 in Bitcoin in the next 24 hours, they would attack his accounts. (Lotich did not pay up, and fortunately the threat turned out to be an empty one.)

SPECIAL OCCASION AND EVENT SCAMS

While fraud happens year-round, scammers often tie it to something timely; maybe it's scams around Valen-

Continued from page 49

The 'Likes For Money' Scam

It starts off with innocuous messages, asking if you want to earn a steady income on the side, without spending much time and effort. All you have to do is to 'like' some videos on YouTube. Click on the links in the message and you get added to a web of Telegram groups, on which you are connected to faceless entities handing over 'tasks' to you—as simple as liking a certain number of YouTube videos in a given duration for a fixed rate. Initially, the 'likes' fetch steady sums of money. But slowly, even as you continue to perform the tasks and earn an income, the money isn't released. Instead, the faceless entities start demanding sums of money to release the pending dues. Before you know it, you've been shaved off massive sums of your savings trying to get your 'dues' back. These fraudsters often also lure unsuspecting victims to 'invest' their money in these operations by promising them hefty returns—as much as 30 to 50 per cent. Prompt payments at the initial stages lulls the victims into trusting the process. In February this year, the daughter of a Lucknow-based businessman lost ₹27 lakhs in such a scam.

The Hospital Appointment Scam:

This cyberscam operates on similar lines as the alcohol-shop scam: through the manipulation of contact details on Google. This scam involves entrapping unsuspecting victims who have searched for the phone numbers of hospitals in order to seek appointments for tests or consultations. As soon as the victims call the number, fraudulent appointments are alloted to them. The catch is, the fraudsters asks the victims to 'confirm' these appointments by paying a small fee. Fraudsters will, then, send a link to victims to complete the payment. Except, as soon as the link is clicked, scammers are able to access the phone and, through it, other confidential details like bank accounts. In February this year, a woman in Mumbai lost ₹1 lakh when she tried to book an appointment at a top city hospital after contacting the establishment through the number listed on Google.

The Utility Bill Payment Scam:

Typically, these scams involve threatening messages to consumers, very often of power companies, warning them that their electric supply would be discontinued if they didn't pay their bills immediately. A payment link, often, accompanies these messages, well-disguised to originate from the power companies. But as soon as a customer clicks on these links, hackers get remote access to their devices and the customers' confidential details are stolen and money is debited from their accounts. In some cases, hackers even ask victims to download apps that can facilitate these 'payments'. Last year, a man from Bengaluru lost ₹4.9 lakh in similar fashion, after receiving a call from a man posing as a representative of his power utility company, asking him to pay up immediately. The man asked him to download TeamViewer Quick Support App, that allowed the hacker remote access to the victim's phone.

—By Kunal Purohit

tine's Day ("Click here to join this 50+ dating site"), tax season ("You're eligible for a refund"), pandemic-related schemes ("Sign up here for free home-testing kits") or war and natural disaster appeals (including phony charities seeking donations).

For example, the CFAC says it received several reports of scams linked to Ukrainian aid in early 2022, when many Canadians were approached over social media to donate money to Ukrainian victims of the war. Instead, these funds went straight into the criminals' pockets.

CRIMINALS POUNCE IN TIMES OF ECONOMIC UNCERTAINTY, AND CAPITALIZE ON NATURAL DISASTERS.

Criminals also take advantage of people in times of economic uncertainty. Facebook users in the US may have seen posts last year from a group called 'Southwest Air Fans' claiming to give away a pair of airline tickets if you clicked on a link to enter a sweepstakes. The perpetrators stole personal information, which led to identity theft.

GRANDPARENT SCAMS

Scammers love to target seniors because they pay so well. Many seniors are hit by fraudsters who send a direct message over social media or via text message posing as their grandchild asking for money due to a medical emergency, a travel problem or to buy textbooks. They glean personal details from the older person's Facebook or Instagram photos, allowing them to craft a very believable message. The caller's phone number looks familiar, so you're more likely to answer (there are computer programmes that let scammers choose the number they want to pop up on your phone).

Often, the 'grandchild' pleads with you to not tell other relatives because they're embarrassed or scared. Wanting to help, the grandparents send money via wire transfer to the scammer.

Regardless of whether or not you are a grandparent, if you get a message like this and it appears to be from a loved one, before sending any money be sure to call the relative directly to ask if they really are in some kind of trouble.

ROMANCE AND 'CATFISHING' SCAMS

Catfishing is when someone pretends to be someone they're not. The fraudster may use a phony name and photo to court someone online, usually over social media—such as Facebook, Instagram or a dating app—with the goal of making the victim fall in love with them. Once trust is obtained, they ask the victim for money.

Rebecca D'Antonio of Orlando, Florida, says she was cheated out of US$100,000 by a man she met online

via an undisclosed dating site. 'Matthew' said he was a widower and a single dad, and after months of building up trust with D'Antonio over email and text messages, he persuaded her to send wire transfers by telling her he needed money for medical bills, or because he had lost his credit card.

HOW TO REDUCE YOUR RISK

All of this may make you want to unplug and go back to the pre-digital age. But it's reassuring to know that the problem is being vigorously tackled by governments and credit-card companies. Even if you're more tech-shy than tech-savvy, you can still protect yourself from cybercriminals. Read on to learn about a few precautions you can take.

USE STRONG PASSWORDS

For all the tech you use, passwords should be at least seven characters long and a combination of letters (upper and lowercase), numbers and symbols. Don't use your birth year or your kids' or pets' names as part of your password. However, a 'passphrase' is a good idea; for example, 'myc@tCis#1!' (derived from 'my cat Charlie is no. 1').

Most importantly, never use the same password for all of your online activity, because if a site or app is breached, then the crooks will try that

same password for your other accounts. Password-manager apps like 1Password and Dashlane can help keep track of all your login information and ensure each password is secure.

PAUSE, DISTRUST, VERIFY

Each time you come across information that requires you to make financial information, follow this three-step process, said Bhatia, the cybersecurity expert. "Firstly, pause, and don't rush into making transactions. Once you pause, inherently distrust anything you read, especially on the internet. Distrust people you speak to or who message you about these transactions. Then, go on to verify whether it could be true or not," said Bhatia. "If you follow these three steps, you will seldom fall into the trap of these cyberfraudsters, adding that these scamsters succeed because they feed on people's "fear, greed and trust."

DON'T ANSWER UNKNOWN VIDEO CALLS

According to Bhatia, you should not respond to video calls by unknown numbers that come your way. You should avoid answering them as far as possible. "But if you must, cover the front camera with your hand and answer it so that your face is not visible to the person on the other end," he said.

DISTRUST INFORMATION ONLINE

Be skeptical of people and information you find online. Do not believe strangers you befriend on the internet. Similarly, when you read something on the internet, take it with a pinch of salt. "I, inherently, believe that everything that Google shows is incorrect. So, I make an effort to verify all the information," Bhatia says.

DON'T PAY FOR JOBS OR SIDE-GIGS

No genuine employer will make an employee pay for a job, nor will a genuine company make an employee pay before releasing their dues. If your employer is asking you to pay up, that's as big a red flag as it can be.

LIMIT THE INFORMATION YOU SHARE

Set your social media profiles to private. If someone asks to connect with you on social media, only accept their request if you know them. Even if it's a name and photo of someone you know, confirm it's them by reaching out to them in another way. If it's a fake, block and report the fraudulent message.

DOUBLE YOUR EFFORTS

For online banking and shopping apps, opt for two-factor authentication, which not only requires your password to log in but also a one-time code sent to your mobile device to prove it's really you.

HIDE YOURSELF

Use the 'private' or 'incognito' mode of your browser, which deletes your history and cookies after your session so the information is not left on the device. Better yet, consider reputable virtual private network (VPN) software to remain anonymous when online.

RETHINK YOUR EMAIL ACCOUNTS

The email accounts you use on social media should not be the same ones you have tied to your bank accounts, health-care information or confidential conversations you may be having, says Payton. "This is because these publicly accessible email accounts can be easily harvested using free marketing tools."

Instead, Payton suggests using an encrypted email platform like Proton Mail, a 'privacy-first' solution. In addition, use separate phone numbers for personal use and anything tied to finances. You can get a free secondary phone number on your existing smartphone from apps like TextNow, Google Voice or Talkatone.

SHOP SAFELY

Always use a secure internet connection—your home Wi-Fi, for example—when making an online purchase. Reputable websites use technologies such as SSL (secure socket layer) that encrypt data during transmission. (You will see a little 'padlock' icon on your browser and usually 'https' at the front of your address bar.) Many cybersecurity experts say it's safer to shop from within a store's app than the web.

Shop only on sites that take secure payment methods, such as credit cards, PayPal, Apple Pay or Google Pay. When shopping at an unfamiliar merchant's site, look for some sort of security seal of approval, such as DigiCert, Better Business Bureau and VeriSign. On auction sites like eBay, check the seller's reputation and read comments before buying a product.

Don't shop (or bank) online using a public Wi-Fi hotspot—such as in a café, airport or hotel lobby—as they're not as secure as your home Wi-Fi or a cellular connection. Instead, make a 'personal hotspot' out of your phone.

PROTECT YOUR TECH

To prevent viruses or other malware, install anti-malware software on your devices. It's like placing a deadbolt on your front door and activating an alarm system. Formerly called anti-virus software, anti-malware software can identify, quarantine, delete and report suspicious activity.

> BE SKEPTICAL OF PEOPLE AND INFORMATION YOU GET ONLINE. WHEN YOU READ SOMETHING ON THE NET, TAKE IT WITH A PINCH OF SALT.

The most robust products include a firewall, encryption options and webcam-intrusion detection (to prevent someone accessing your webcam).

Protection against scams is about being on guard, learning to sense when something seems suspicious and installing software, such as anti-malware, to give you peace of mind. R