Cybersecurity:

How to help your clients protect their business

Presented by **Mastercard**

Hosted by **Association of Women's Business Centers**

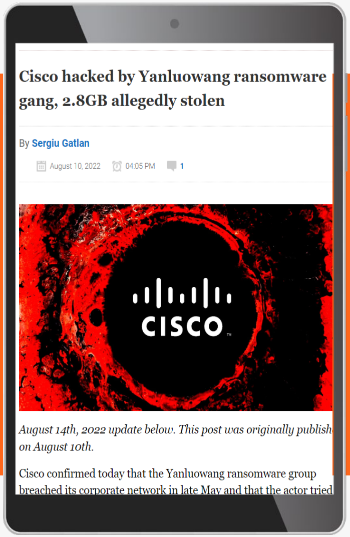
Presenter, Gina Ganahl, PhD, VP, Product Management, Mastercard Trust Center, Cyber & Intelligence at Mastercard

July 26, 2023

Session Topics

Cybersecurity trends, threats, best practices and free resources to help protect your business

The headlines can be scary!



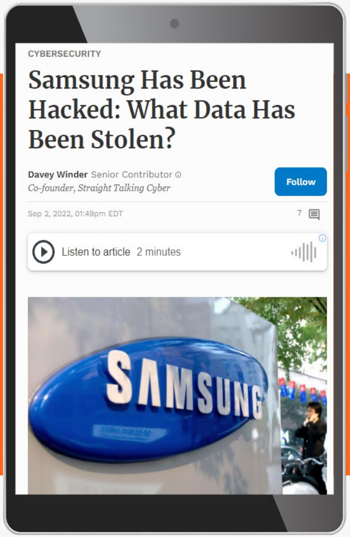
Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen

By Sergiu Gatlan

August 10, 2022 04:05 PM 1

August 14th, 2022 update below. This post was originally publish on August 10th.

Cisco confirmed today that the Yanluowang ransomware group breached its corporate network in late May and that the actor tried



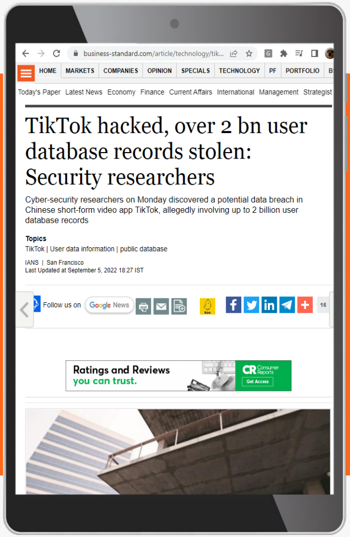
CYBERSECURITY

Samsung Has Been Hacked: What Data Has Been Stolen?

Davey Winder Senior Contributor

Co-founder, Straight Talking Cyber

Sep 2, 2022, 01:49pm EDT 7



business-standard.com/article/technology/tik...

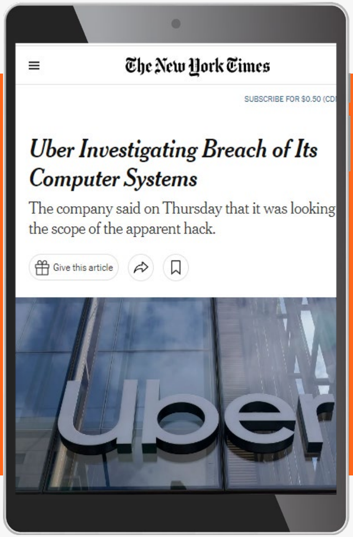
TikTok hacked, over 2 bn user database records stolen: Security researchers

Cyber-security researchers on Monday discovered a potential data breach in Chinese short-form video app TikTok, allegedly involving up to 2 billion user database records

Topics

TikTok | User data information | public database

IANS | San Francisco
Last Updated at September 5, 2022 18:27 IST



The New York Times

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking the scope of the apparent hack.

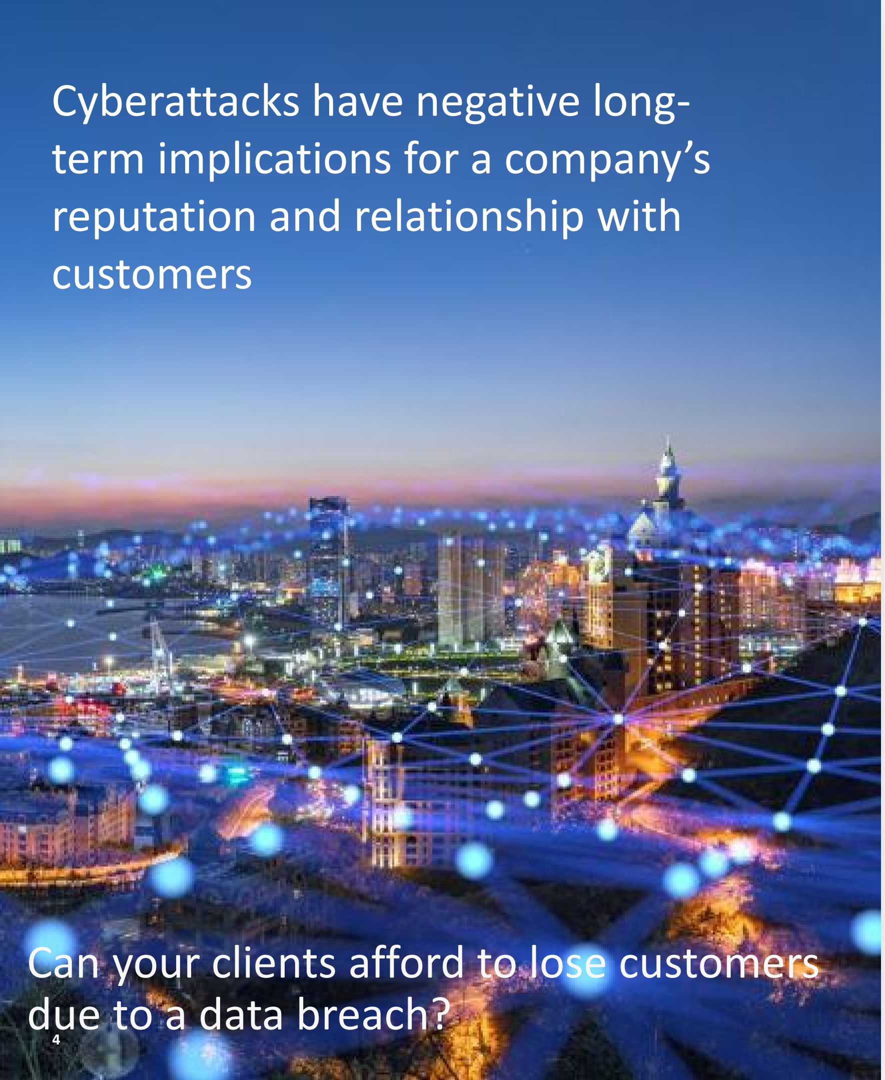
46% of companies will be hit with some form of virus or malware[1]

90% of companies will experience a phishing attack[1]

27% of companies will be hit by ransomware[1]

27% of companies will be affected by a business email compromise[1]

[1] Aite (2023), Threat research is based 30 independent threat reports curated and analyzed

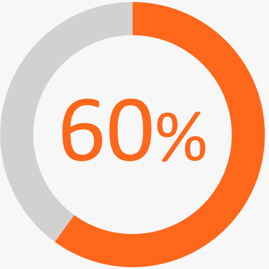


Cyberattacks have negative long-term implications for a company's reputation and relationship with customers

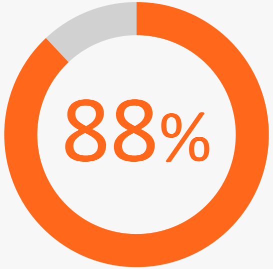
Can your clients afford to lose customers due to a data breach?

#1

Security and privacy safeguards are the most important factor for consumers when deciding to do business with a company



of consumers are unlikely to shop with companies that have a significant data breach



of customers won't use a brand they don't trust with data[1]

Sources:
The Great Data Exchange, Become 2020.
1. https://techwireasia.com/2021/02/customers-are-losing-patience-with-data-security-issues/

Mastercard is committed to helping small businesses mitigate cyber risk

The consequences of failing to take proactive cybersecurity actions can be disastrous.

Let’s explore actions your clients can take to help improve cybersecurity

> *“It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.”*
>
> **Stephane Nappo**
> Global Head Information Security,
> Société Générale International Banking

Let’s focus on 6 key topics for cybersecurity culture change for your clients’ businesses

Authentication

Data Backup and Recovery

Software Updates

Phishing

Ransomware

USBs

Source: Adapted from the Cyber Readiness Institute’s Cyber Readiness Starter Kit https://cyberreadinessinstitute.org/starter-kit/

#1. Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.[1] Goal: Make it difficult for fraudsters to gain access to protected resources.

63%

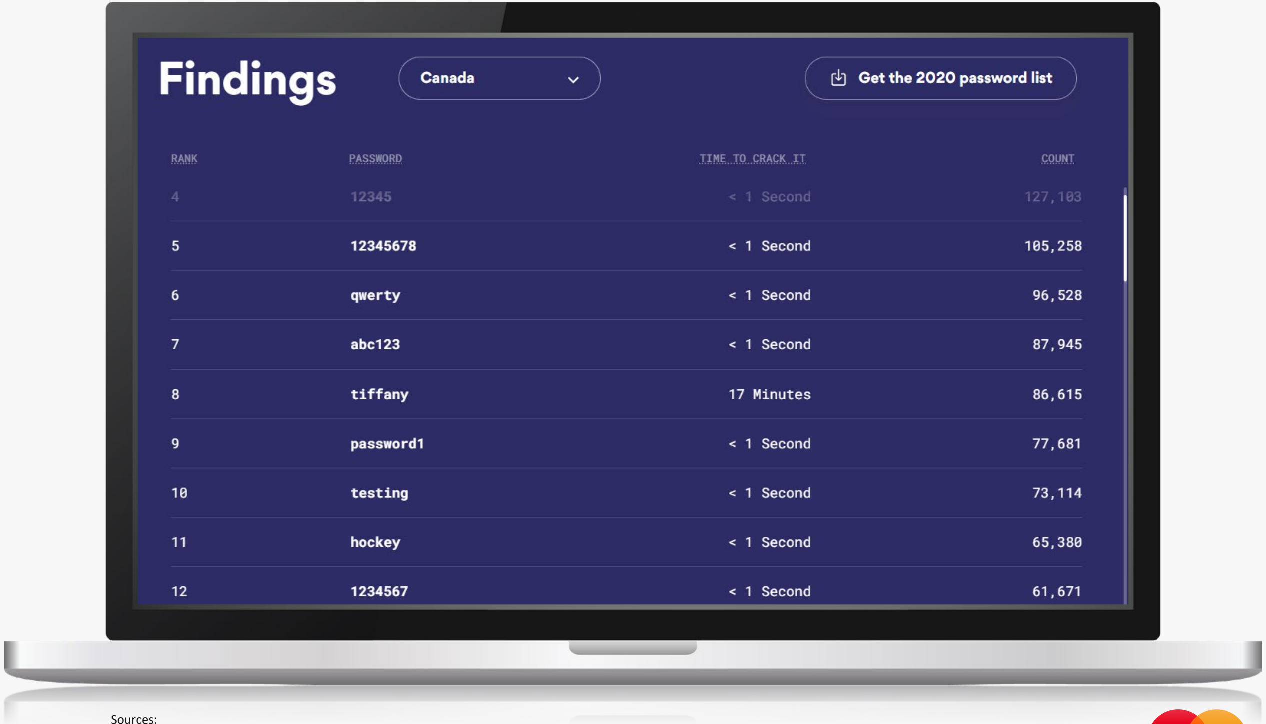
of data breaches result from weak or stolen passwords[2]

23M

people use password 123456. This takes less than a second to crack[3]

50%

of people use the same password for all their logins[3]



Findings

RANK	PASSWORD	TIME TO CRACK IT	COUNT
4	12345	< 1 Second	127,103
5	12345678	< 1 Second	105,258
6	qwerty	< 1 Second	96,528
7	abc123	< 1 Second	87,945
8	tiffany	17 Minutes	86,615
9	password1	< 1 Second	77,681
10	testing	< 1 Second	73,114
11	hockey	< 1 Second	65,380
12	1234567	< 1 Second	61,671

Sources:
1. National Institute of Standards and Technology
2. Cyber Readiness Institute
3. Web Tribunal (2023) Impressive Password Statistics to Know in 2023

Authentication: Solutions

✓ Strengthen your passwords or passphrases with 14 to 16+ characters that include a combination of upper- and lower-case letters, numbers, and characters.

Learn more: Beyond Simple Passwords video

✓ Never reuse passwords on multiple accounts

✓ Never share passwords with others

✓ Use a trusted, secure password manager application

✓ Enable two-factor authentication:

- Two-factor requires you to input a unique code that is sent to your mobile device for each new login.
- Two-factor authentication creates an important security link between the password and the person.

Learn more: Multi-Factor Authentication article

#2. Data backup and recovery

21%

of ransomware attacks are backup systems targeted until they were unusable[1]

Data backup and recovery is the process of creating and storing backup copies of data to safeguard businesses from data loss due to breaches, external attacks, software crashes and hardware failures.[2]

Solutions

✓ Separate the backup infrastructure from the active directory (Active Directory is a database that stores and organizes enterprise resources as objects.)

- Backup data on an external hard drive and store it in a locked, fire/waterproof location
- Or use cloud storage or an online backup service

✓ Since ransomware attacks often propagate on the same operating system, it may be worthwhile to adopt a different operating system for the backup infrastructure

✓ To further reduce the risk of an administration account being compromised, backup administration access should also be strengthened, for example with multi-factor authentication (MFA).

Learn more: Data Backup & Recover video & tools

Sources:
[1] https://www.riskinsight-wavestone.com/en/2021/11/cyber-attacks-what-are-the-risks-for-backups-and-how-to-protect-yourself/
[2] https://fluentpro.com/blog/top-7-advantages-of-data-backup-and-recovery/

#3. Software updates

60%

of attacks in 2019 exploited gaps in software already on computers[1]

A software update or patch is a set of changes to an operating system, program, app or its supporting data designed to update, fix or improve it. This includes fixing security vulnerabilities and other bugs.

Failure to patch systems in a timely fashion can leave your operations vulnerable and exposed.

Sources:
1. Ponemon (2019_ Ponemon Institute Vulnerability Survey

Software updates: Solutions

When you receive a notification to update to the latest version of your software or operating system, it’s best to update right away

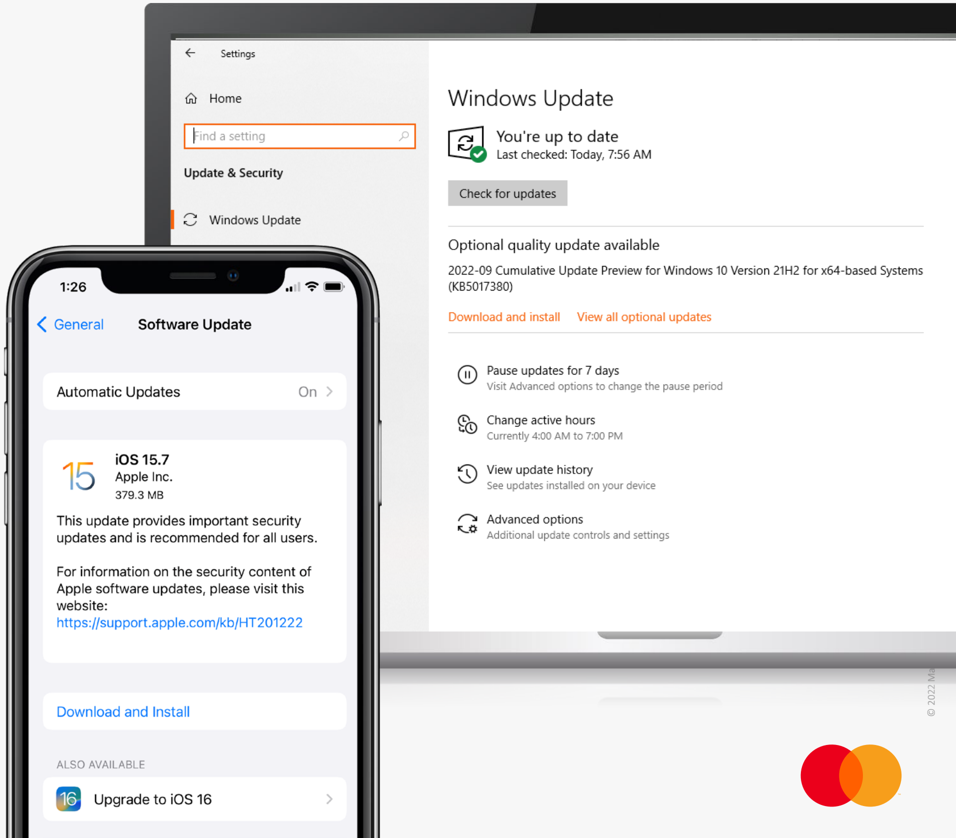
- Turn on the auto updates whenever it is offered
- A best practice is to assign one person to manage updates for all company computers

Updates are issued often for programs like Microsoft Word and Excel, as well as your computer operating system like Windows or MacOS

Update all software and apps

- On your business and personal devices
- Both those issued by the company and those downloaded by employee
- These updates often include security patches

Learn more: Patching Essentials



Windows Update

You're up to date
Last checked: Today, 7:56 AM

Check for updates

Optional quality update available

2022-09 Cumulative Update Preview for Windows 10 Version 21H2 for x64-based Systems (KB5017380)

Download and install View all optional updates

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 4:00 AM to 7:00 PM

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

Automatic Updates On

iOS 15.7
Apple Inc.
379.3 MB

This update provides important security updates and is recommended for all users.

For information on the security content of Apple software updates, please visit this website:
https://support.apple.com/kb/HT201222

Download and Install

ALSO AVAILABLE

Upgrade to iOS 16

#4. Phishing

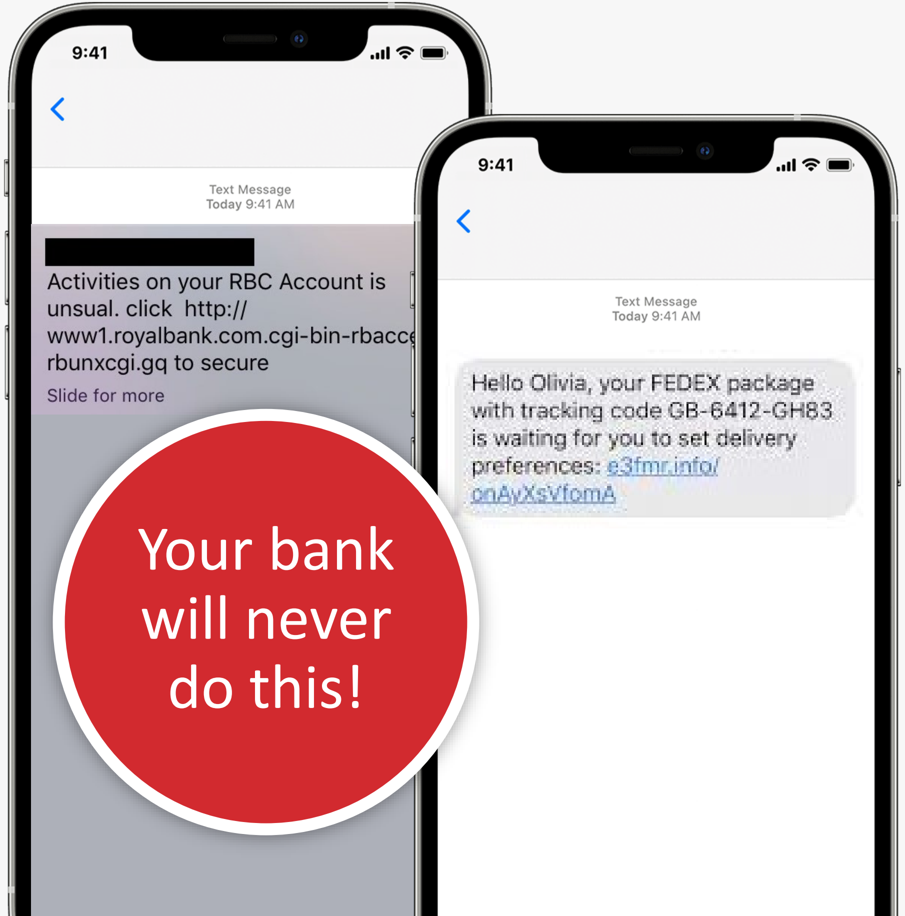
91%

of all cyberattacks start with a phishing email[1]

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. The goal is to steal sensitive data like credit card, PII, and login information, or to install malware on the victim's machine.

A phishing email may look like a real message.
But opening it may result in downloading software viruses or giving attackers access to your data.

Once you have been caught in a phishing net, your systems may become infected with malware, a type of ransomware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.



[redacted]
Activities on your RBC Account is unsual. click http:// www1.royalbank.com.cgi-bin-rbacc rbunxcgi.gq to secure
Slide for more

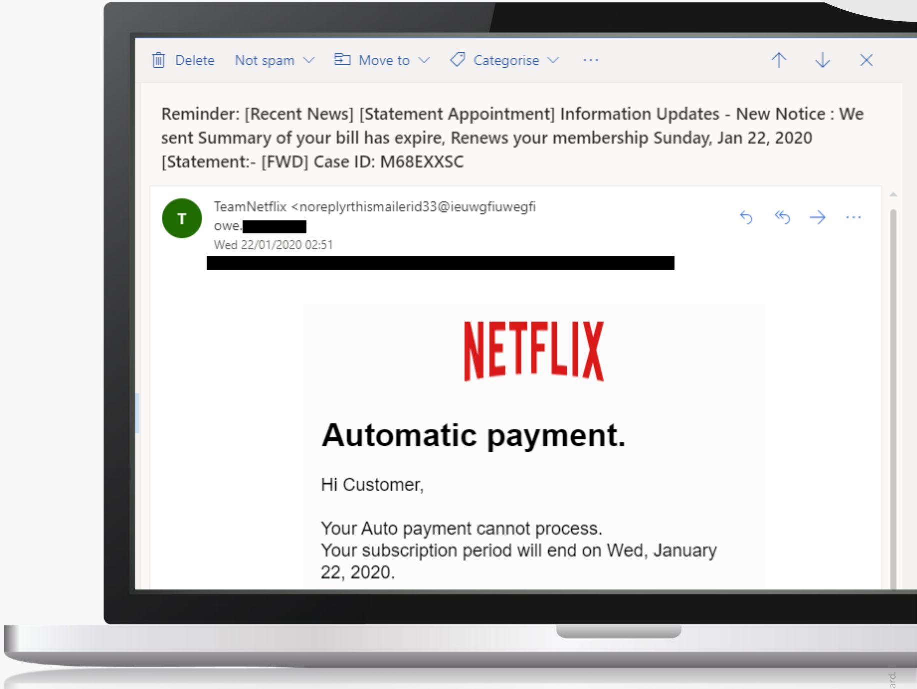
Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/ onAyXsVfomA

Your bank will never do this!

Sources:
[1] Cyber Readiness Institute

Phishing: Solutions

- ✓ Check the sender’s email address and any other identifying information (e.g., company logo, address and contact details) for any inconsistencies, miss spellings, or signs it may be fake.
  - Details may often look similar but be slightly off
- ✓ If you are not familiar with the email sender, do not click any links or download any attachments in the email.
  - Call the customer service phone number found on the supposed sender’s website to seek information.
- ✓ Delete any suspicious emails and immediately empty your trash. Inform employees of the suspicious email.
- ✓ Back up data often in case your data is taken hostage.
- ✓ Ask yourself, “Do I know you (the sender) like that?”



Reminder: [Recent News] [Statement Appointment] Information Updates - New Notice : We sent Summary of your bill has expire, Renews your membership Sunday, Jan 22, 2020 [Statement:- [FWD] Case ID: M68EXXSC

TeamNetflix <noreplyrthismailerid33@ieuwgfiuwegfi
owe.[redacted]
Wed 22/01/2020 02:51
[redacted]

Automatic payment.

Hi Customer,

Your Auto payment cannot process.
Your subscription period will end on Wed, January 22, 2020.

Learn more: [Protecting Your Small Business: Phishing video]

[Phishing Prevention video]

#5. Ransomware

- Ransomware is a form of malware that infects your computer or device.
- When ransomware takes control of your computer or device, it locks you out of that computer, device or certain files entirely.
- The bad actors will require a lot of money from organizations to get their critical assets and information back.
- Business as usual is locked down until you can access your data

Solutions

✓ Avoid suspicious downloads, as cyber criminals commonly spread ransomware through email attachments, infected programs and compromised websites.

✓ Regularly back up your files.

✓ Keep your operating system updated.

✓ Contact No More Ransom.org if your business is hit with a ransom attack

NO MORE RANSOM!

#6. USBs and removable media

27%

of malware infections originate from infected USBs[1]

USB drives can be useful for sharing files between computers, but they can also be used to deliver viruses and malware. There's no way to tell where the drive has been or who may have compromised it.

Solutions

✓ Introduce easy-to-use alternatives to USB drives, such as cloud-based file-sharing services so that USB drives are less necessary.

✓ Use good judgment: If you don't know where the drive came from, don't plug it in.

Sources:
1. Cyber Readiness Institute

Review: Best practices and tips

- ✓ Use two-factor authentication whenever available
- ✓ Don’t reuse the same passwords across multiple sites
- ✓ Use strong passwords

- ✓ Keep software up to date with the latest patches
- ✓ Consider automatic updates when available
- ✓ Back your data up regularly
- ✓ Share data in the cloud rather than USBs to enhance security

- ✓ Avoid clicking on links and attachments in emails
- ✓ If you weren’t expecting the email, verify using a trusted phone number
- ✓ Don’t be rushed by a sense of urgency in the message
- ✓ Listen to your gut: If something feels off, delete the message

- ✓ Register for Mastercard Identity Theft Protection, it’s **free** for Mastercard credit card holders

Protect. Detect. Alert. Resolve.

An Iris Powered by Generali service

How to report cyberattacks and helpful resources

- File a police report with your local police department or sheriff’s office.
- Check with your state’s law enforcement office and Attorney General for any required reporting.
  - This is especially important to comply with data breach reporting requirements.
- File a complaint with the FBI’s Internet Crime Complaint Center (IC3).
- Leverage resources, you are not alone.

cybercrime SUPPORT NETWORK

NO MORE RANSOM

NATIONAL CYBERSECURITY ALLIANCE

SBA U.S. Small Business Administration

Report Internet Crime to the FBI www.ic3.gov

Mastercard Trust Center

The Trust Center is a microsite on Mastercard.com websites.

We offer free access to cybersecurity education, resources, and tools designed to help small and midsize businesses (SMBs) secure their digital ecosystem.

Why is cybersecurity important for your business?

- **90%** of SMBs will experience a phishing attack[1]
- **83%** of SMBs are not financially prepared to recover from a cyberattack[2]
- **46%** of SMBs will be hit with some form of virus or malware[1]

Sources: 1. Aite-Novarica Group (2023). 2. Cybersecurity Magazine (May 2021).

Visit the Mastercard Trust Center to learn how to improve the security of your digital ecosystem

Cybersecurity learning journeys to fit every level of expertise

LEARN THE BASICS

"I'm a beginner who's feeling overwhelmed"

EXPAND YOUR KNOWLEDGE

"I'm fairly experienced but want to learn more"

MASTER YOUR SECURITY

"I'm an expert looking to keep one step ahead"

Resources include

PODCASTS | VIDEOS | WHITEPAPERS | ARTICLES | INFOGRAPHICS | TOOLKITS

Click here to start learning today!

Additional **Free** Cybersecurity Education Resources

CYBER READINESS INSTITUTE

- Visit Cyber Readiness Institute
- Visit Cyber Readiness Starter Kit
- Visit Cyber Readiness Program
- Visit Cyber Leader Certification Program

GLOBAL CYBER ALLIANCE

- Visit Global Cyber Alliance: Enabling a Secure and Trustworthy Internet
- Visit GCA Cybersecurity Toolkit For Small Business

NATIONAL CYBERSECURITY ALLIANCE

- Visit Stay Safe Online
- Visit Resources & Guides
- Visit Events & Programs

NO MORE RANSOM!

- Visit No More Ransom
- Visit Prevention Advice
- Visit Report a Crime

HSB Cyber Insurance

Mastercard and HSB have partnered to bring you cyber insurance and peace of mind to withstand a potentially devastating cyberattack.

- √ Comprehensive cyber risk insurance coverage for 5 pervasive cyber threats included in every policy
- √ Provides tailored policies, customizing limits and deductibles plus optional coverage enhancements are available to meet each small business's needs
- √ Leverages RiskRecon's My Cyber Risk assessments to present a comprehensive view of each small business's cyber security posture
- √ Offers competitive pricing and dynamic premium adjustments based on the small business cybersecurity profile

DATA BREACH

FRAUD

IDENTITY THEFT

COMPUTER ATTACK

CYBER LIABILITY

Learn more and get protected today at [HSB Total Cyber]

Mastercard is not an insurance advisor or provider of insurance and does not act as a third-party adjuster or claims assessor for any party. Coverage is provided by The Hartford Steam Boiler Inspection and Insurance Company. Terms, conditions and exclusions apply. Purchase Street Insurance Services, LLC ("PSIS") is a licensed P&C insurance agency which is a wholly-owned subsidiary of Mastercard. PSIS receives compensation based on certain insurance policies sold by HSB. Further information is available upon request. State insurance licenses (including but not limited to): Arkansas insurance license: #100165620, California insurance license: #0M65062, Minnesota insurance license: #40501033, Oklahoma insurance license: #3000426648 and Texas insurance license: #2176453.

Questions?

Contact me:

Gina.Ganahl@Mastercard.com