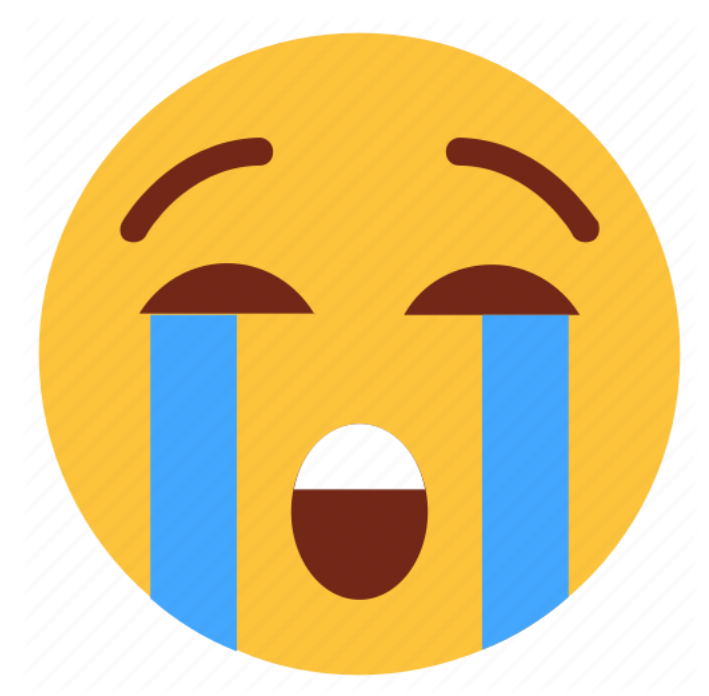


STAY SAFE IN ONLINE SHOPPING

BILLY CHUANG
SOLUTION ENGINEERING MANAGER
NORTH ASIA
CYBERARK SOFTWARE





WHAT DO YOU LOSE ?



HKTV
mall



amazon

ebay



ebay

PChome^{ONLINE}



KICKSTARTER

citiesocial 找 好東西

INDIEGOGO

Branding
Reputation


Product
Quality




Payment


Delivery


FACEBOOK AD/POST


 Smowow

贊助 · 

This smart massager uses both heat and low-frequency electrical pulse technology to relieve neck & shoulder pains and reduce stress. Can be taken anywhere to enjoy a well deserved relaxation session.



 繼續播放影片

 瞭解詳情
smowow.com

Useful at work, while travelling, or relaxing at home

SMOWOW.COM

The Smart Neck Massager


瞭解詳情



smowow


smowow.com/?fbclid=IwAR0x59IVqDl(TC)3RdKyETWUuXpRAGamhp65zeK4ZVv83ndNgSVgJD2Mo

Apps Work CyberArk Software ARJ - ARJ - Confu... WhatsApp Demo_Client_PAS... Alarm_SplashScreen Facebook Yahoo! 香港 MyPortal BillyLink

Free Worldwide Shipping TODAY!

 Home Smowow™ Track Your Order



Discover Smowow™

The World's Smartest Neck Massager

GET IT NOW!

FACEBOOK AD/POST



Useful links

Privacy Policy

Refund Policy

Terms and Conditions

Contact

contact@smowow.com

Newsletter

SUBSCRIBE

AMEX

Apple Pay

Google Pay

MasterCard

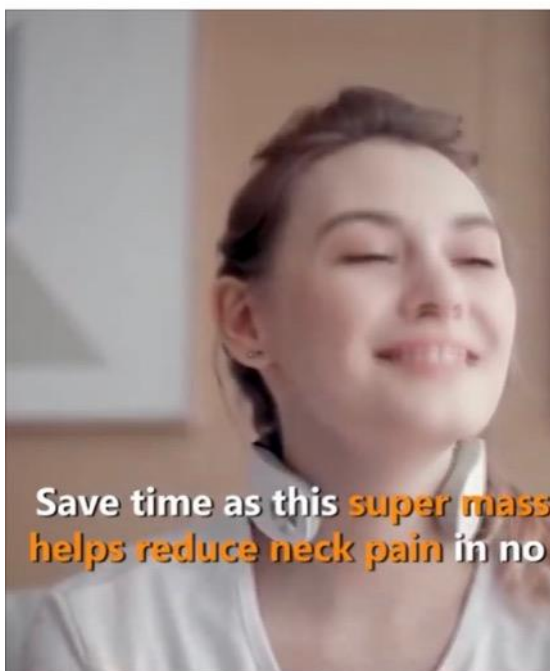
Paycom

OPay

VISA



Get relief from the neck pain with our
SUPER MASSAGER 😍
... Continue reading

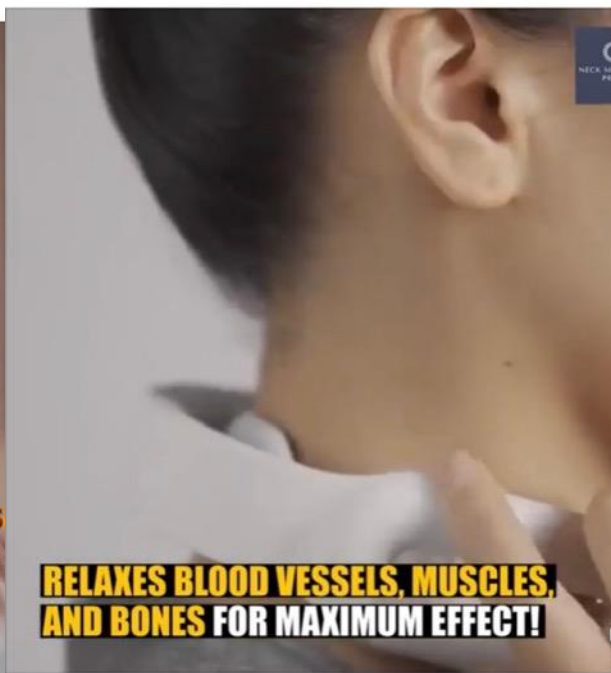


Save time as this **super mass**
helps reduce neck pain in no

THESERIC.COM
✓ **REDUCE NECK PAIN**
50% OFF + FREE SHIPPING



Say **NO MORE** to expensive chiropractor and
massage bills with the Neck Massager Pro™
... Continue reading



**RELAXES BLOOD VESSELS, MUSCLES,
AND BONES FOR MAXIMUM EFFECT!**

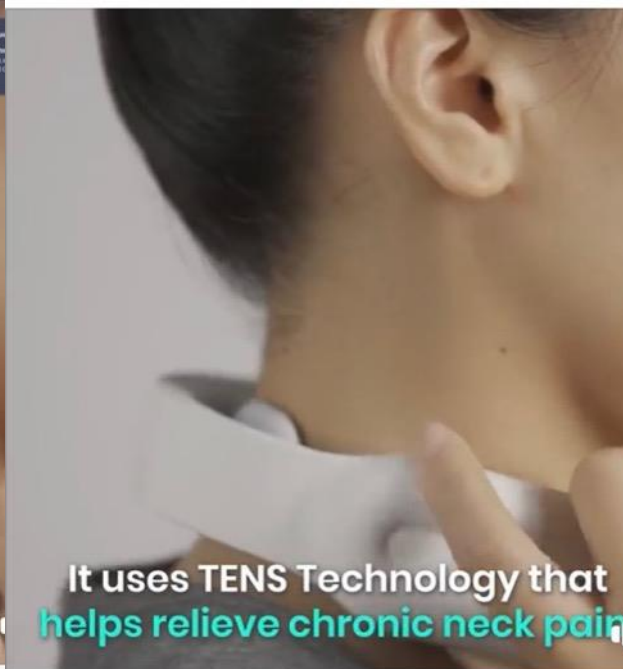
NECKMASSAGERPRO.COM
Neck Massager Pro™

Shop

Like Comment Share



Treat yourself to your own personal neck
massager
... Continue reading



It uses TENS Technology that
helps relieve chronic neck pain

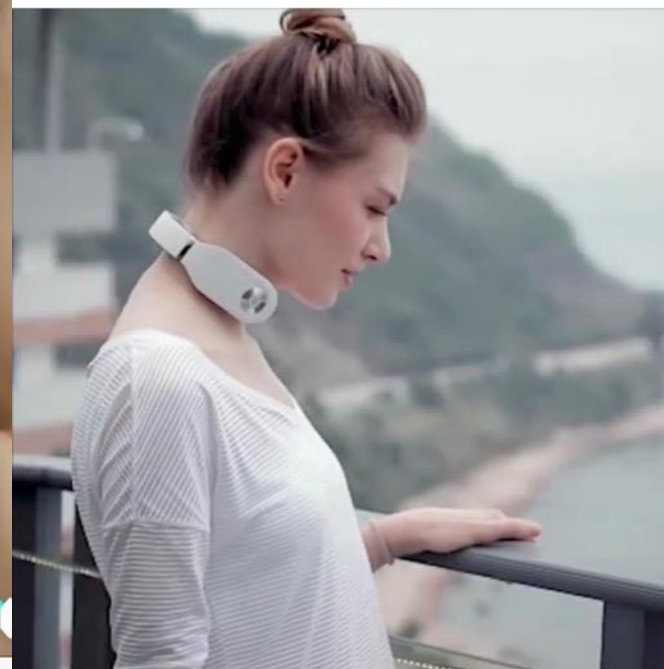
KNOTSAWAY.CO
KnotsAway Massager

Shop Now

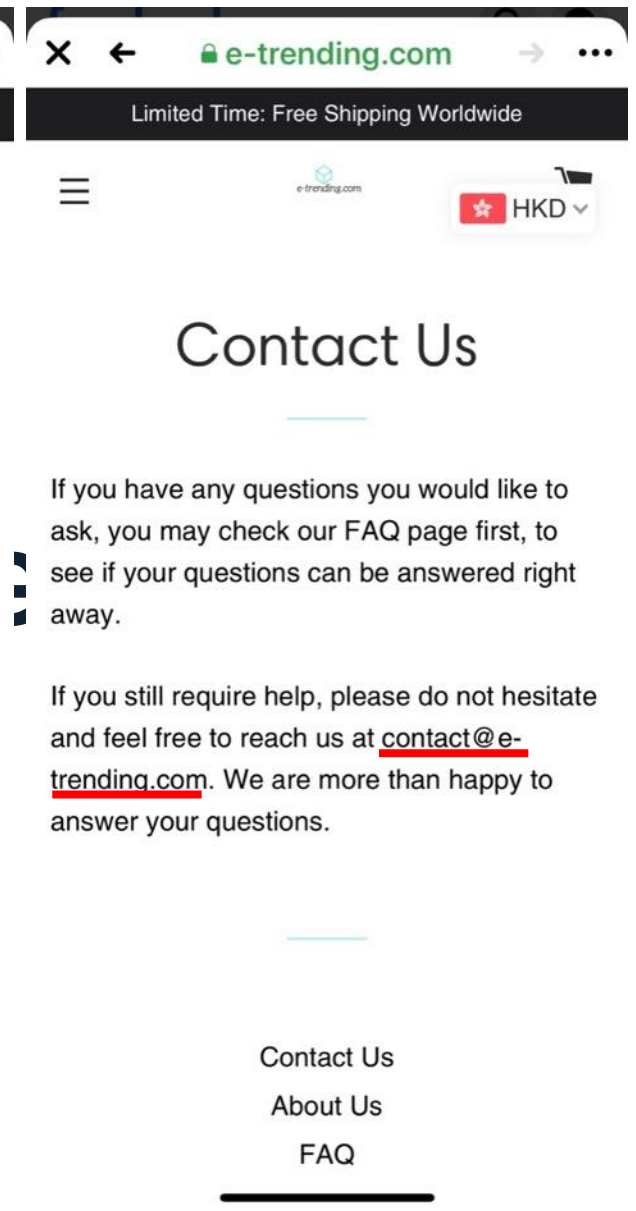
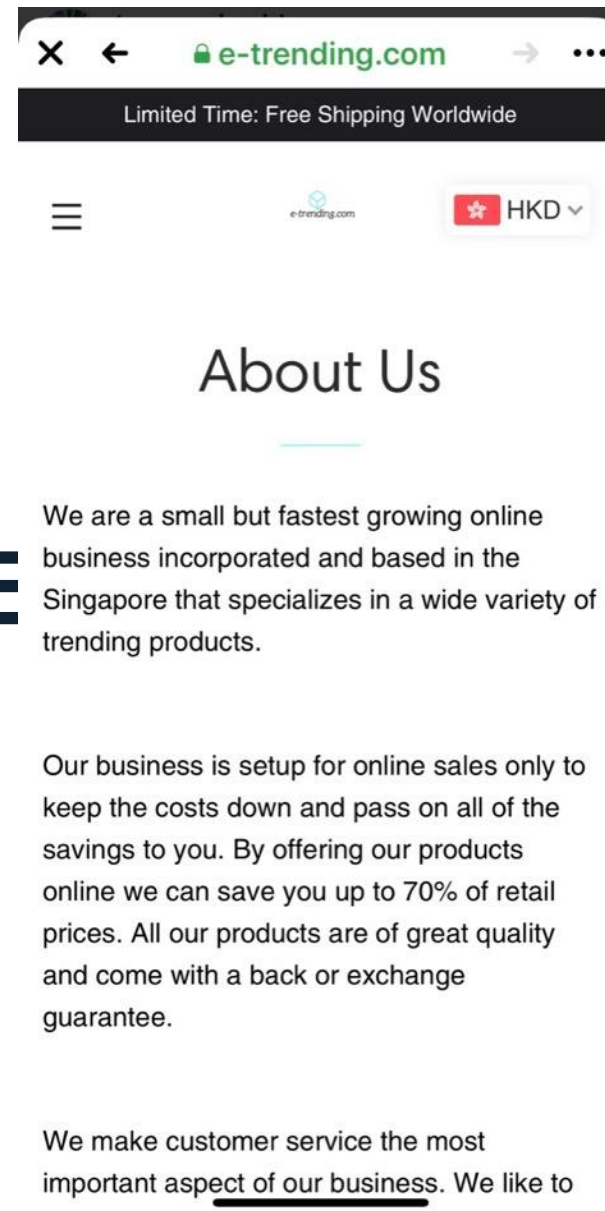
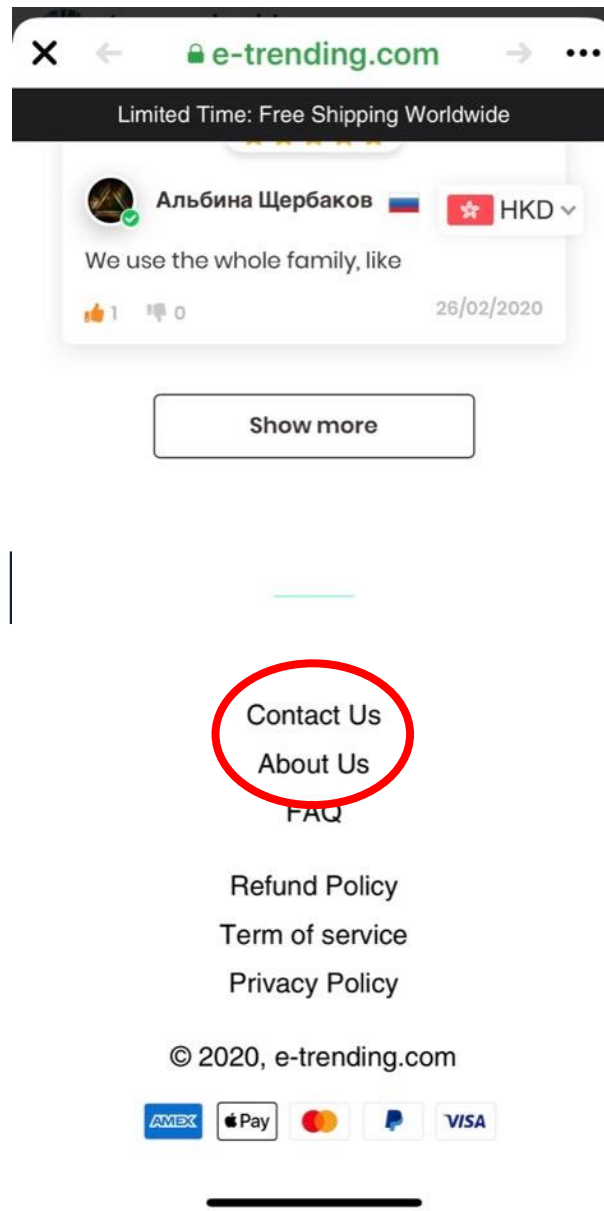
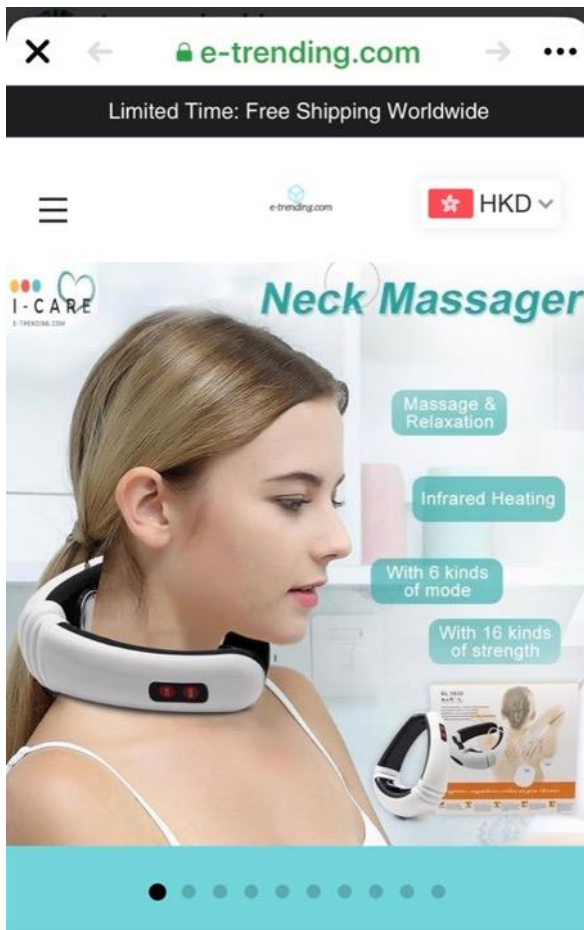
Shop Now




Cervical Vertebra Massager Instrument
Cervical Spine Home. 🖱️ Buy it now ➡️ <https://bit.ly/2WcViIB>



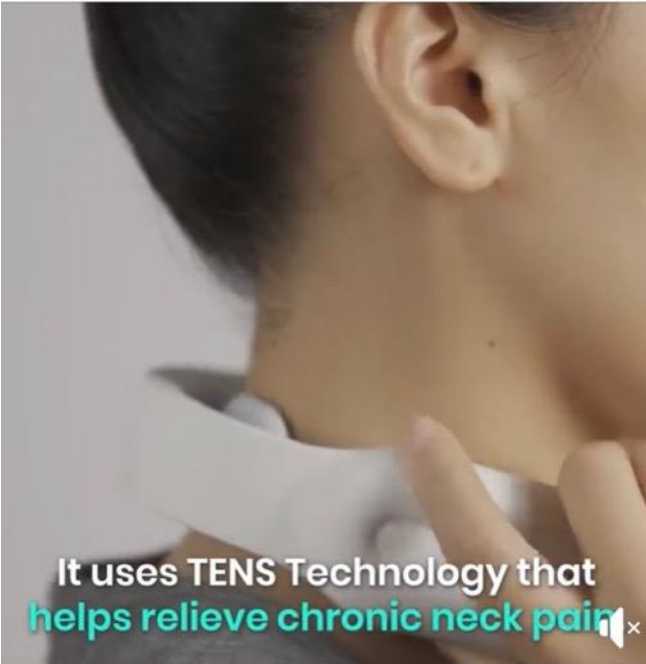
CTRLYOUR.COM



ANOTHER EXAMPLE

 **KnotsAway**
Sponsored · 🌐

Treat yourself to your own personal neck massager
... Continue reading






It uses TENS Technology that helps relieve chronic neck pain

KNOTSAWAY.CO
KnotsAway Massager

Shop Now

Free Shipping on All Orders!

KNOTSAWAY 🔍 👤 🛒 ☰



Vanessa from Hobbs, New Mexico
Recently bought KnotsAway™ Massager!
Verified by Proof Factor

knotsaway.co

Show more reviews

Quick links

- About
- Privacy Policy
- Refund Policy
- Shipping Policy
- Terms of Service

knotsaway.co


KnotsAway™ is an innovative brand dedicated to bringing electrical stimulation products. We launched our first product in 2019, and took the internet by storm.

We have designed the **most convenient solution** for **stress, chiropractic manipulation**, and **prolonged straining**. Using **electrical nerve stimulation as well as the heated function**, the KnotsAway™ Band promotes blood circulation, relieving cervical pain and stiffness, all while providing a Therapeutic & Stimulating effect.


Our main priority is YOU, our customers. If you have any issue with your order, or if you have a question about our product, feel free to contact us by email at support@KnotsAway.co

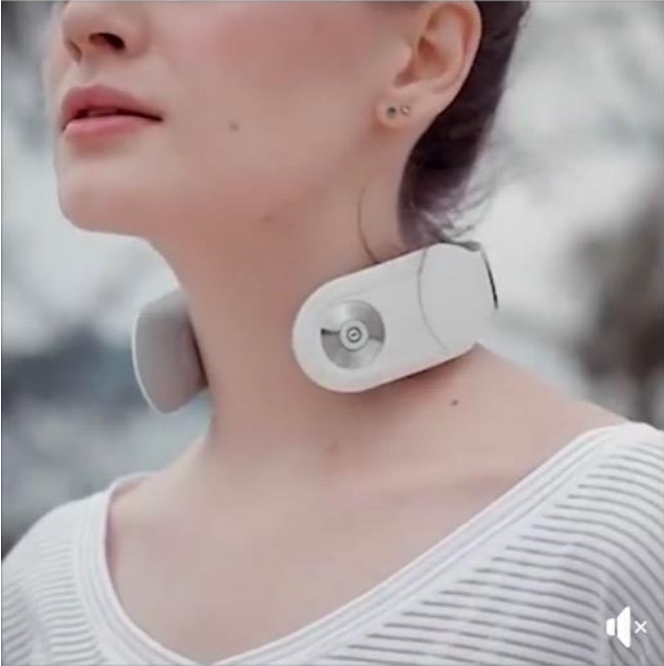
We look forward to solving all your Neck problems! Follow us on your favorite social media platform for our latest updates:

PROCESS TO PAYMENT




CtrlYour-Ins
Sponsored · 🌐






 **Cervical Vertebra Massager Instrument**
Cervical Spine Home.👉 Buy it now ➡️ <https://bit.ly/2WcViLB>







CTRLYOUR.COM


 **Cervical Vertebra Massager Instrument**

Shop Now

   www.ctrlyour.com  

 **CTRLYOUR**  

Size: One Size 

Color: Same Picture Color 

-

1







+




ADD TO CART

BUY IT NOW

[View product details](#)


© CTRLYOUR





^

TOP

 CYBERARK



11

Contact	<input type="text"/>	Change
Ship to	<input type="text"/>	Change
Method	FREE Worldwide Shipping · Free Change	

Payment

All transactions are secure and encrypted.

☒ Credit card


VISA  AMEX  and more...

Card number

Name on card

Expiration date (MM / YY)

Security code

☐ 

Billing address

Select the address that matches your card or payment method.

☒ Same as shipping address

☐ Use a different billing address

Remember me

☐ Save my information for a faster checkout

[Return to shipping](#)

Pay now

暖頸同時可以按摩：溫熱EMS按摩頸環

<https://www.mayngan.com/products/mytrex-ems-neck-massager>

當你覺得凍嘅時候，其實只要確保頸、足部係暖嘅，其實成個身體就會變暖🔥🔥上次去鹿兒島嘅時候，見到呢個「溫熱EMS按摩頸環」即刻去試，其實本身想買頸巾，但最後決定買咗呢個溫熱EMS按摩頸環。點解？因為我一路行街可以暖頸嘅同時，其實都順便做埋按摩。平時頸部係最需要按摩嘅身體部位，因為我哋平時耷低頭、望電腦不知不覺令到頸部（人體最脆弱嘅肌肉）長期繃緊，咁最好就當然係一路按摩、一路暖頸啦！



MAYNGAN.COM
mytrex ems

來去逛逛

mayngan.com/products/mytrex-ems-neck-massager?fbclid=IwAR0It_b3HKSSM8syxj6PEsxnCvzoL...

Facebook 專頁 熱賣產品 最新上架 日本直送 旅遊產品 減肥產品 美容保養 抗疫系列 營友會員優惠 所有商品

全部商品 / 預購產品

Mytrex EMS 溫熱頸部按摩器 (日本直送)

全店，買滿\$600免運費(港澳地區)

HK\$699.00 HK\$899.00

(現貨 - 付款後 5-7 個工作天發貨)

數量: 1

現在預購

加入追蹤清單

分享到: 93

商品描述

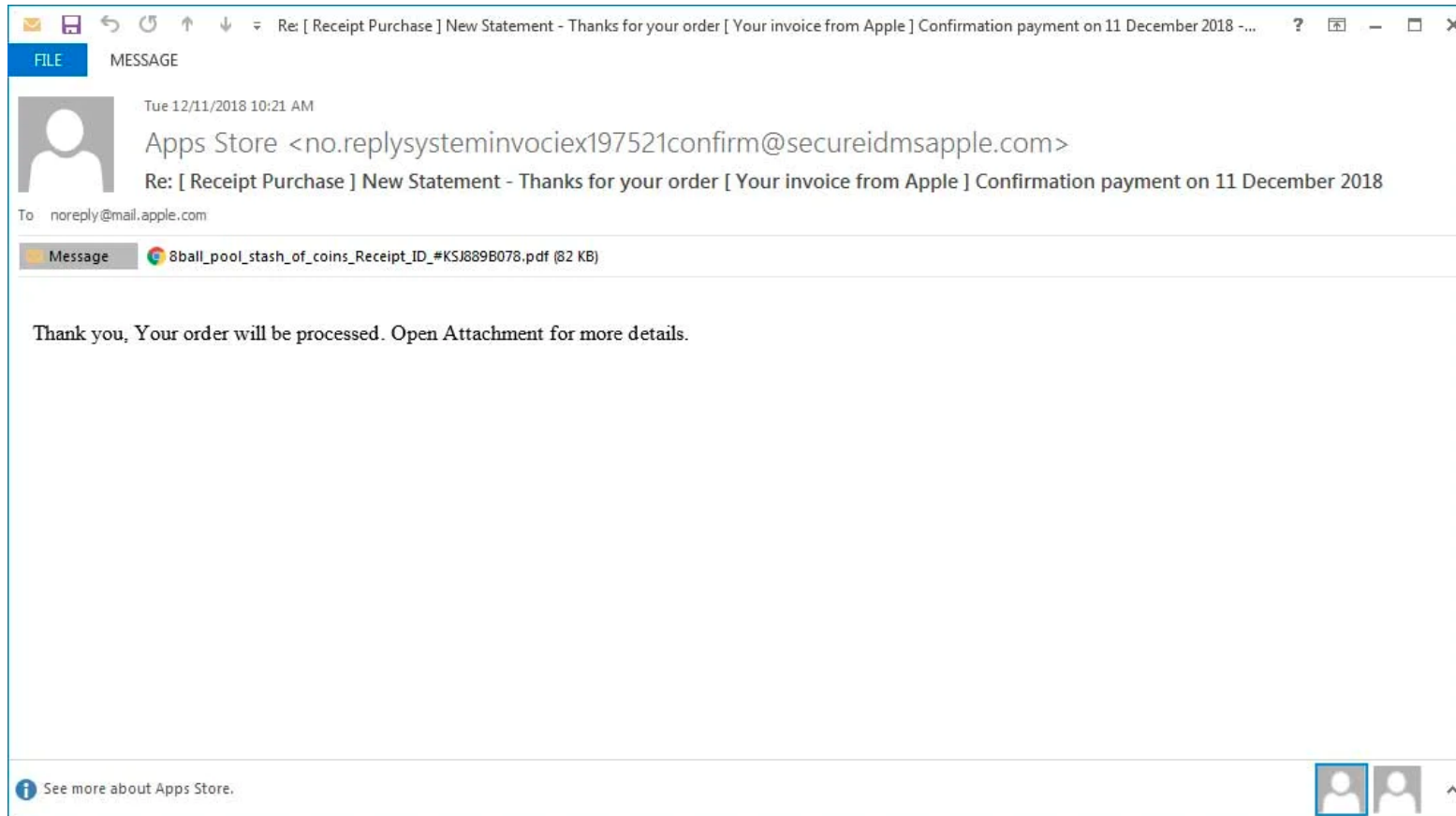
送貨及付款方式

May I Keep Young
歡迎光臨！如有任何問題，歡迎與我們聯絡。

回覆至 May I Keep Y...

FAKE EMAIL AND PHISHING WEBSITE

WIDESPREAD APPLE ID PHISHING ATTACK PRETENDS TO BE APP STORE RECEIPTS



Resource: <https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/>

FAKE EMAIL AND PHISHING WEBSITE

WIDESPREAD APPLE ID PHISHING ATTACK PRETENDS TO BE APP STORE RECEIPTS

The image shows a screenshot of a web browser displaying a fake Apple receipt. The receipt is titled "Tax Invoice" and includes the Apple logo. It contains the following information:

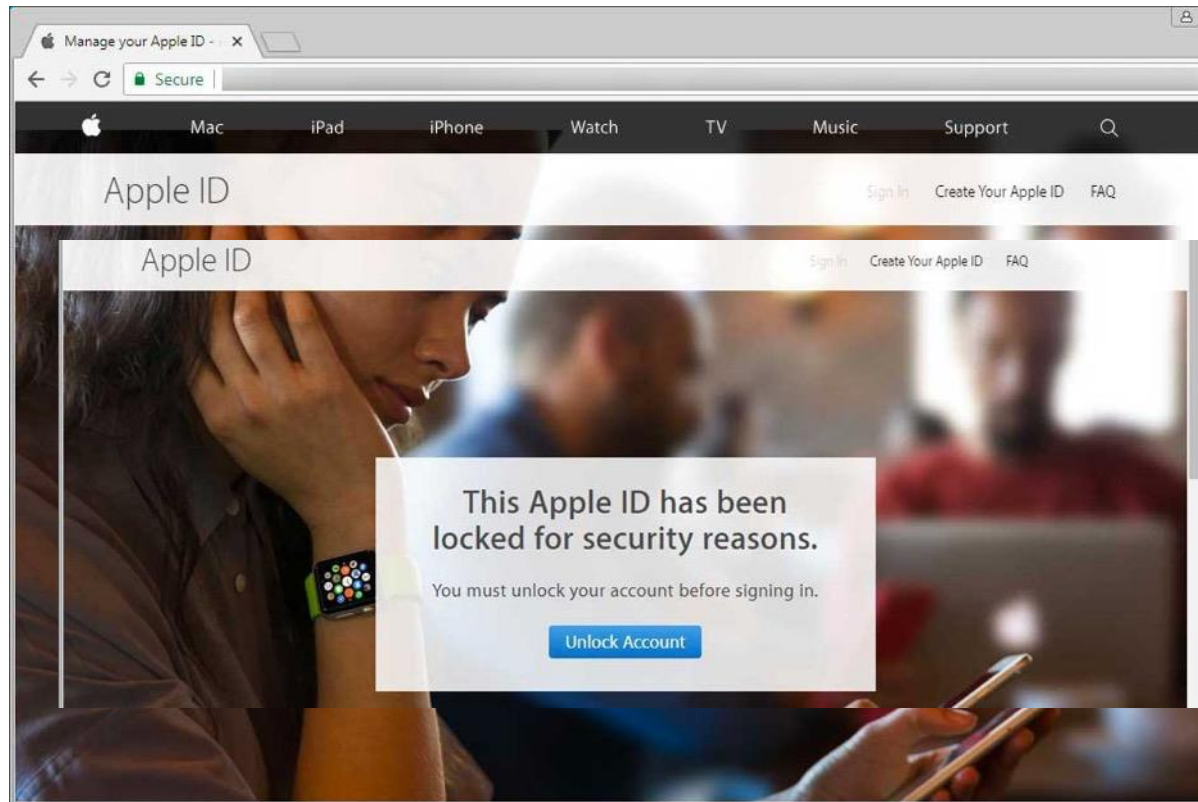
- Thanks to Purchasing!
- DATE: 11 December 2018
- ORDER ID: [KSJ889B078](#)
- DOCUMENT NO.: 135116838084
- BILLED TO: Credit Card, Diego Corrie, 88/1160 creek rd, Carina Heights, QLD 4152, AUS
- TOTAL: \$30.99

The receipt lists a purchase from the App Store:

App Store	TYPE	PURCHASED FROM	PRICE
8 Ball Pool™, Stash of Coins Report a Problem	In-App Purchase	iPhone	\$30.99
TOTAL			\$30.99

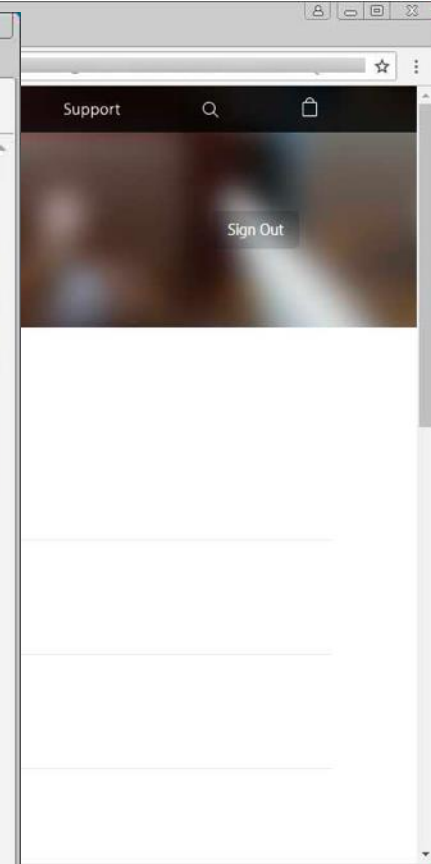
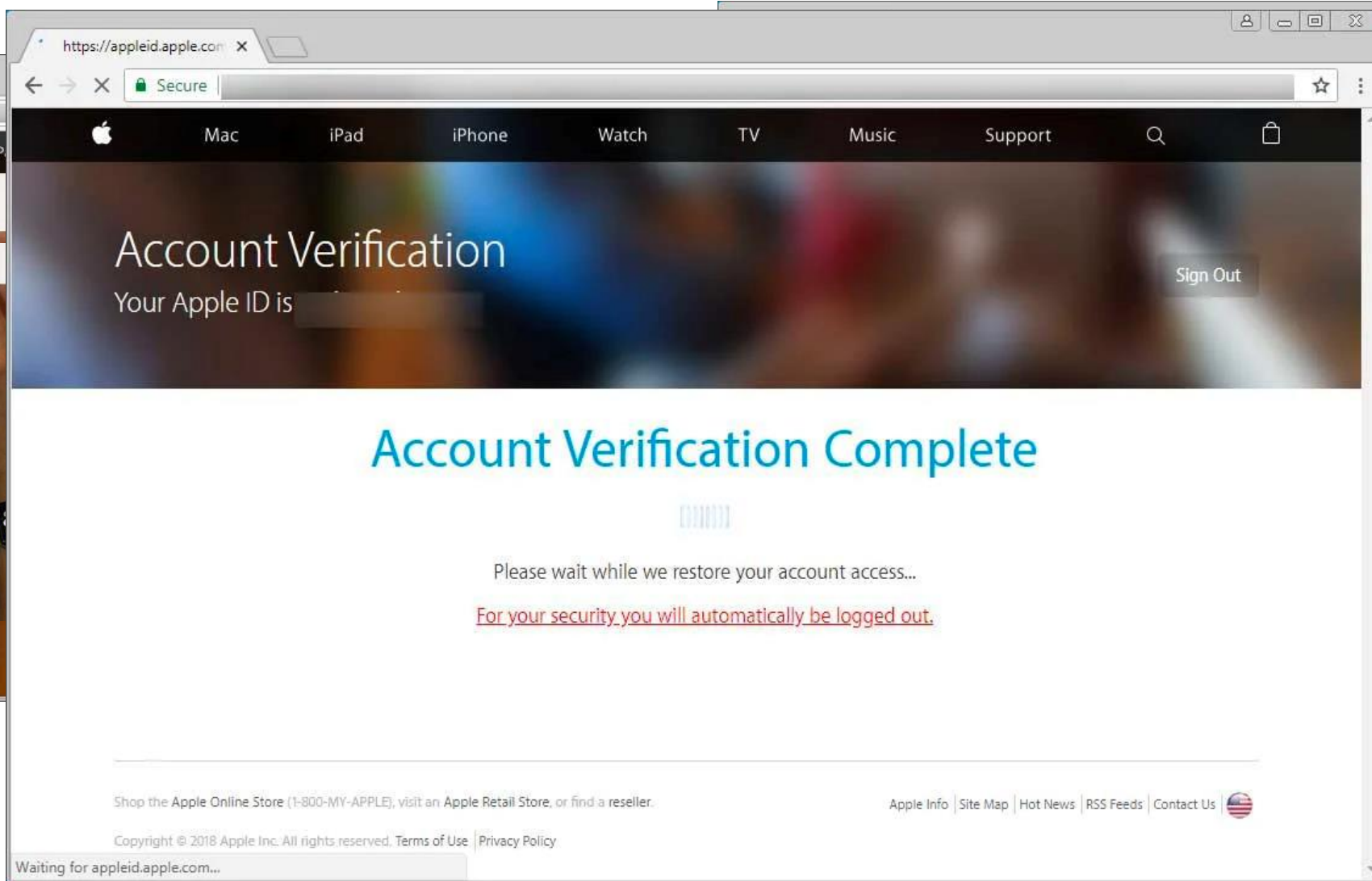
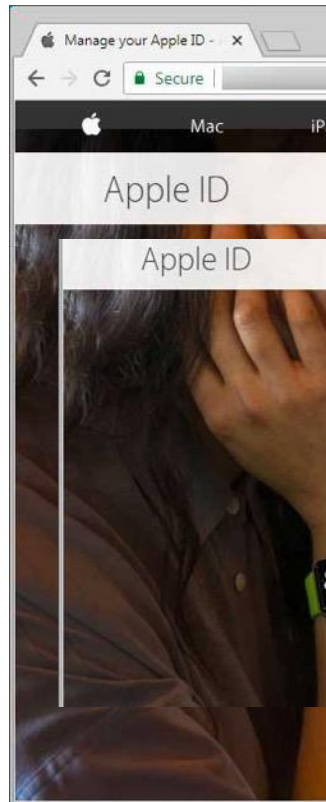
At the bottom of the receipt, there is a section titled "Issues with this transaction?" with the text: "If you haven't authorized this transaction, click the link below to get full refund: <http://idmsa.apple.com/IDMSWebAuth/signin?orderId=KSJ889B078>". A red arrow points from this link to a larger, magnified view of the link on the right side of the image. The magnified view shows the link <http://idmsa.apple.com/IDMSWebAuth/signin?orderId=KSJ889B078> circled in black. The text "Issues with this transaction?" is also visible in the magnified view.

Resource: <https://www.bleepingcomputer.com/news/security/widespread-apple-id-phishing-attack-pretends-to-be-app-store-receipts/>

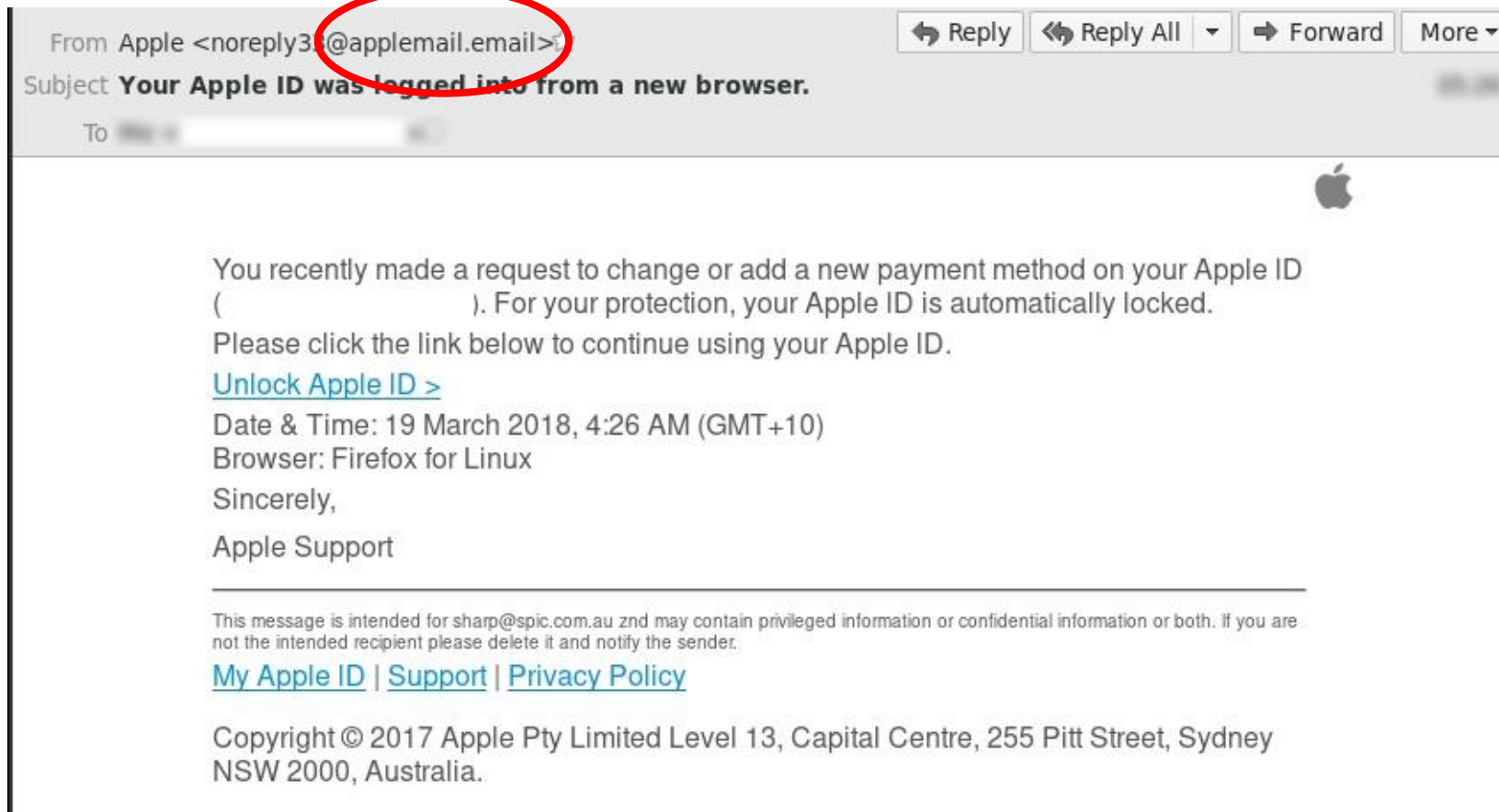


A screenshot of a web browser displaying the Apple ID account verification page. The browser's address bar shows "Confirm your information" and "Secure". The page features a navigation bar with links for Mac, iPad, iPhone, Watch, TV, Music, and Support. Below the navigation bar, the text "Account Verification" is displayed, followed by "Your Apple ID is" and a blurred ID number. A "Sign Out" link is visible in the top right corner. The main content area is titled "Personal Informa..." and contains several input fields for personal information:

- NAME
 - first name
 - middle name (optional)
 - last name
- DATE OF BIRTH
 - date of birth
- TELEPHONE
 - telephone number
- SOCIAL SECURITY NUMBER
 - social security number

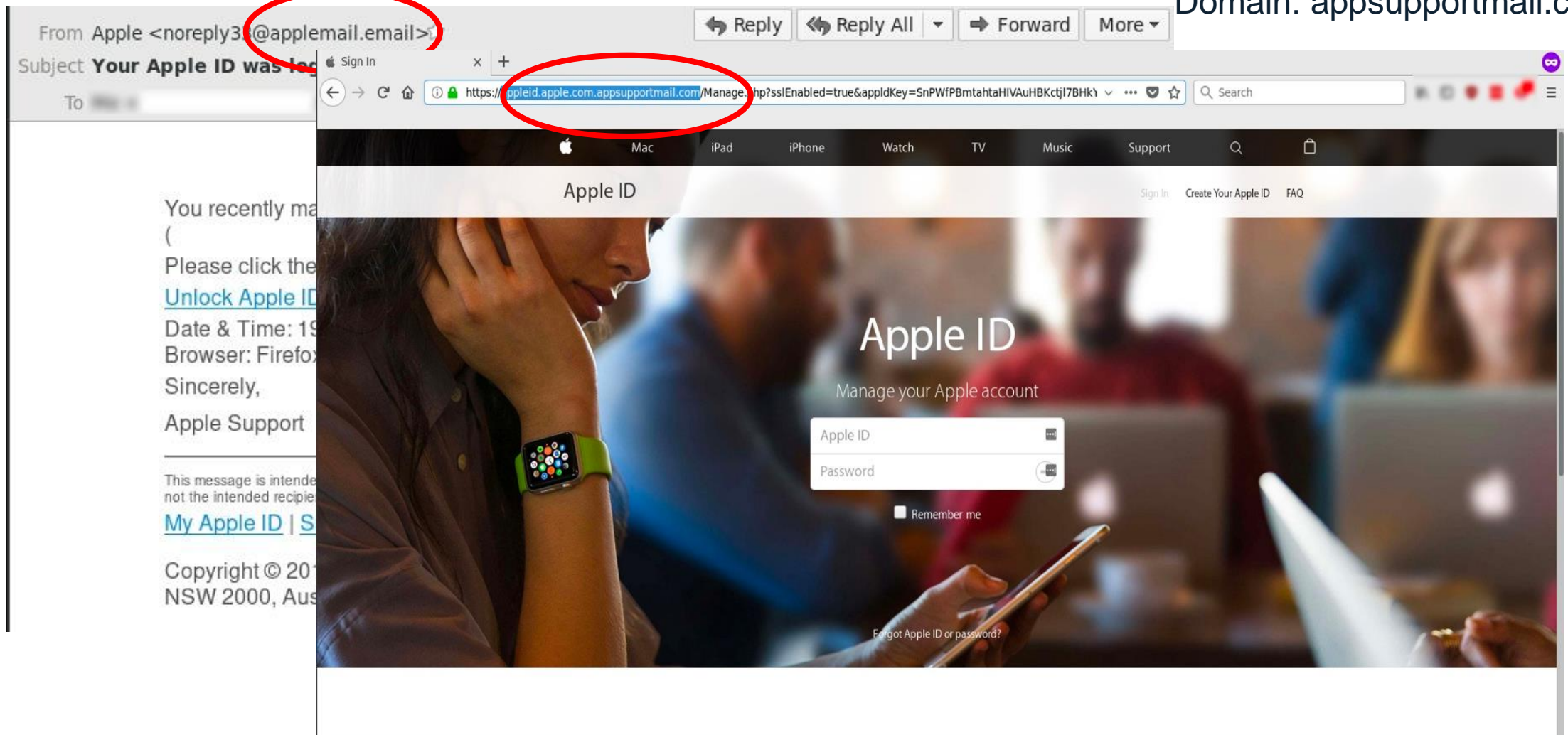


domain: applemail.com

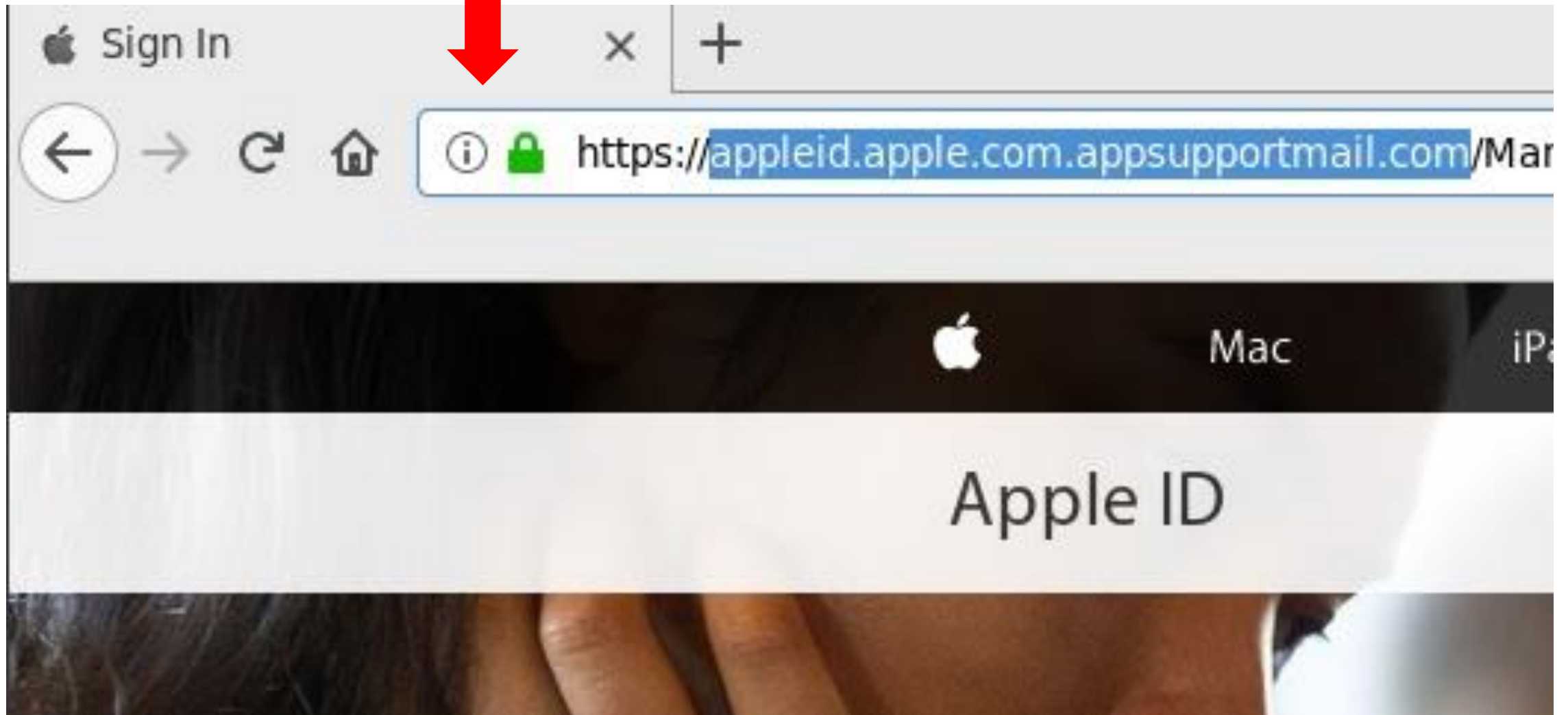


domain: applemail.com

Host: applied.apple.com
Domain: appsupportmail.com



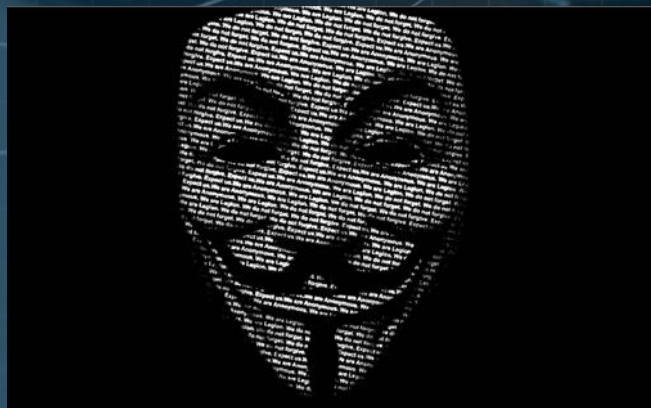
appleid.apple.com.appsupportmail.com



Most **attacks** start on the endpoints



Regardless of origin, attacker will typically have restricted rights and will need to elevate privilege to achieve goal (e.g. financial or data theft, disruption, vandalism)



CREDENTIAL THEFT



PRIVILEGED CREDENTIALS

Bloomberg [Subscribe](#)

Cybersecurity

Uber Hack Shows Vulnerability of Software Code-Sharing Services

Forbes

Grasping The Problem With Privileged Accounts

USA TODAY Privileged Account: The Master Keys Hackers Know Best

One big reason cyber intruders can easily roam far and wide, once they crack inside a company network, is that many organizations pay scant heed to privileged..

CNBC

The Capital One breach is unlike any other major hack, with allegations of a single engineer wreaking havoc

FINANCIAL TIMES

Retail sector

England's NHS hit by large scale cyber attack

CNN BUSINESS

Every single Yahoo account was hacked - 3 billion in all

CBS NEWS

"WannaCry" ransomware attack losses could reach \$4 billion

New Credential-Theft Attack Weaponizes DNS 8/30/2019 02:10 PM **DARK Reading**

The recently discovered campaign sends stolen data out of the network as part of a DNS query.

A new credential-theft attack campaign is using DNS to exfiltrate data. The

cyberscoop

TECHNOLOGY

Russian government hackers used office technology to try to breach privileged accounts

MONTREAL GAZETTE

Desjardins: Rogue employee caused data breach for 2.9 million members

Help Net Security October 10, 2019

Impact and prevalence of cyberattacks that use stolen hashed administrator credentials

InformationWeek DARK Reading

Watch the Watchers: 'Trusted' Employees Can Do Damage

BizTech

NIST Creates New Guidelines for Managing Privileged Accounts

Privileged Account Details Are Often Shared and Can Be a Weak Entry Point for Attackers

SECURITYWEEK

Privileged Account at Root of Most Data Breaches

If enterprises ever were given wake-up call, it should be this; stealing and exploiting privileged accounts is a critical success factor for attackers in 100% of all...

info security

The New York Times

Attack Gave Chinese Hackers Privileged Access to U.S. Systems

THE WALL STREET JOURNAL

Malware Targets Vulnerable Admin Accounts

CSO

Privileged Comes with Peril in World of Cybersecurity

Security experts have been warning enterprises for some time that the greatest security...

SC MAGAZINE

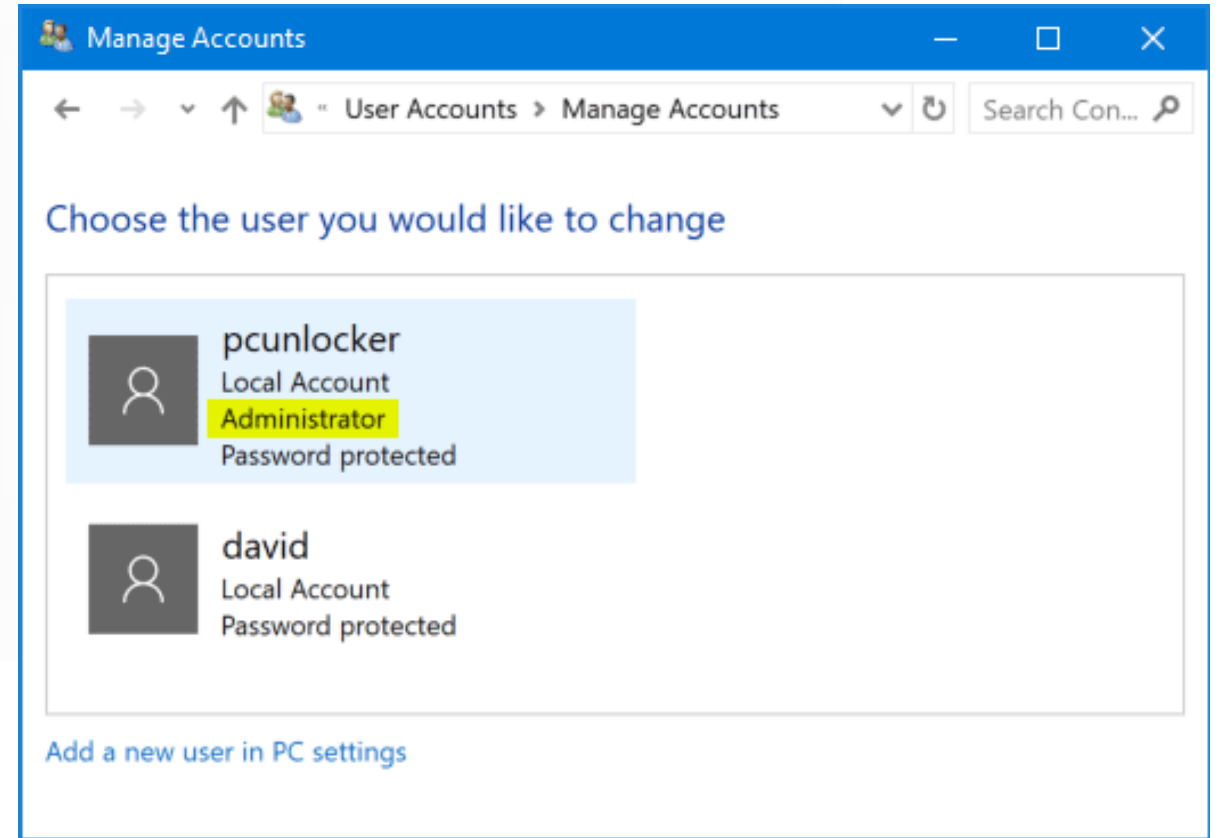
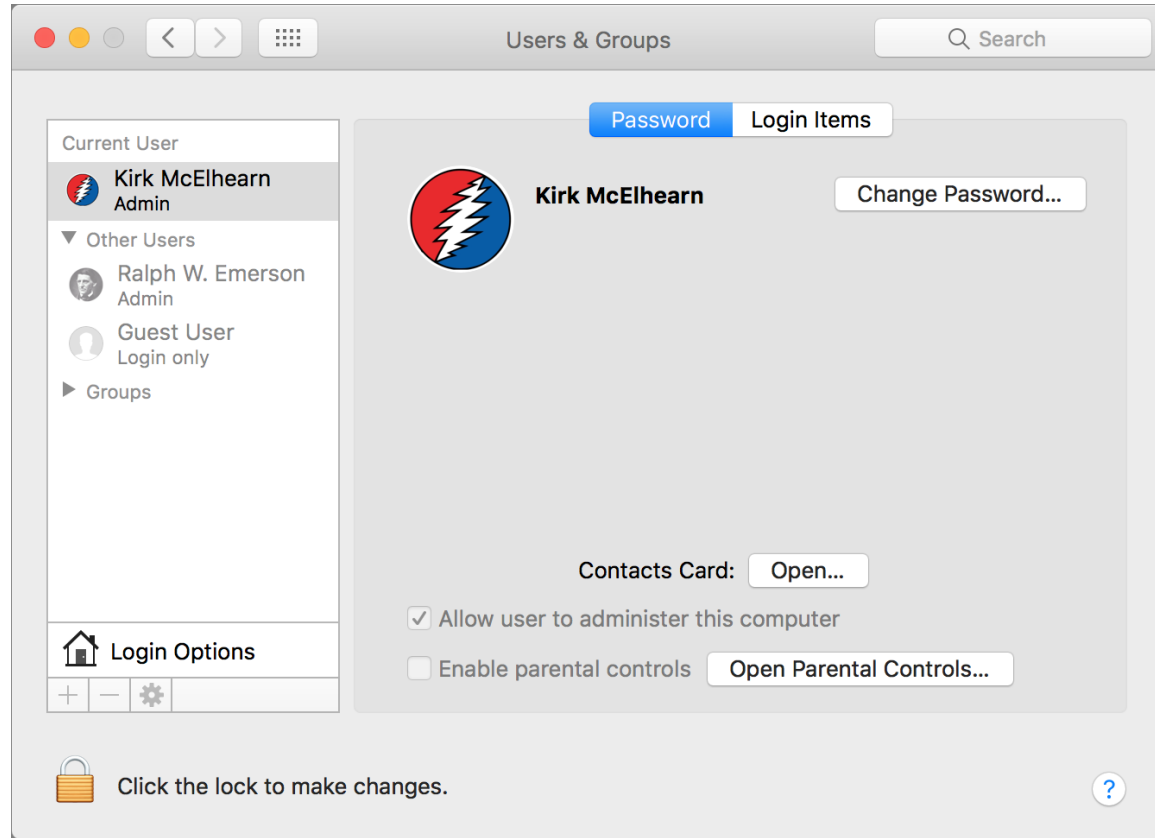
Privileged Account Details Are Often Shared and Can Be a Weak Entry Point for Attackers

verizon

Annual Data Breach Investigations Report

The use of stolen credentials still leads the way from a hacking variety standpoint...

ENDPOINTS – THIS IS WHERE IT STARTS



STANDARD VS LOCAL ADMIN RIGHT



SECURITY VS OPERATIONAL



OPERATIONS IMPACT



SECURITY IMPACT

USERS HAVE LOCAL ADMIN RIGHTS

Happy,
productive users



LOCAL ADMIN RIGHTS ARE REMOVED

Increased burden on
the support team.
Increased calls and costs.



Increased
security incidents



Contain attacks
on the endpoint



RANSOMWARE ATTACK



Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

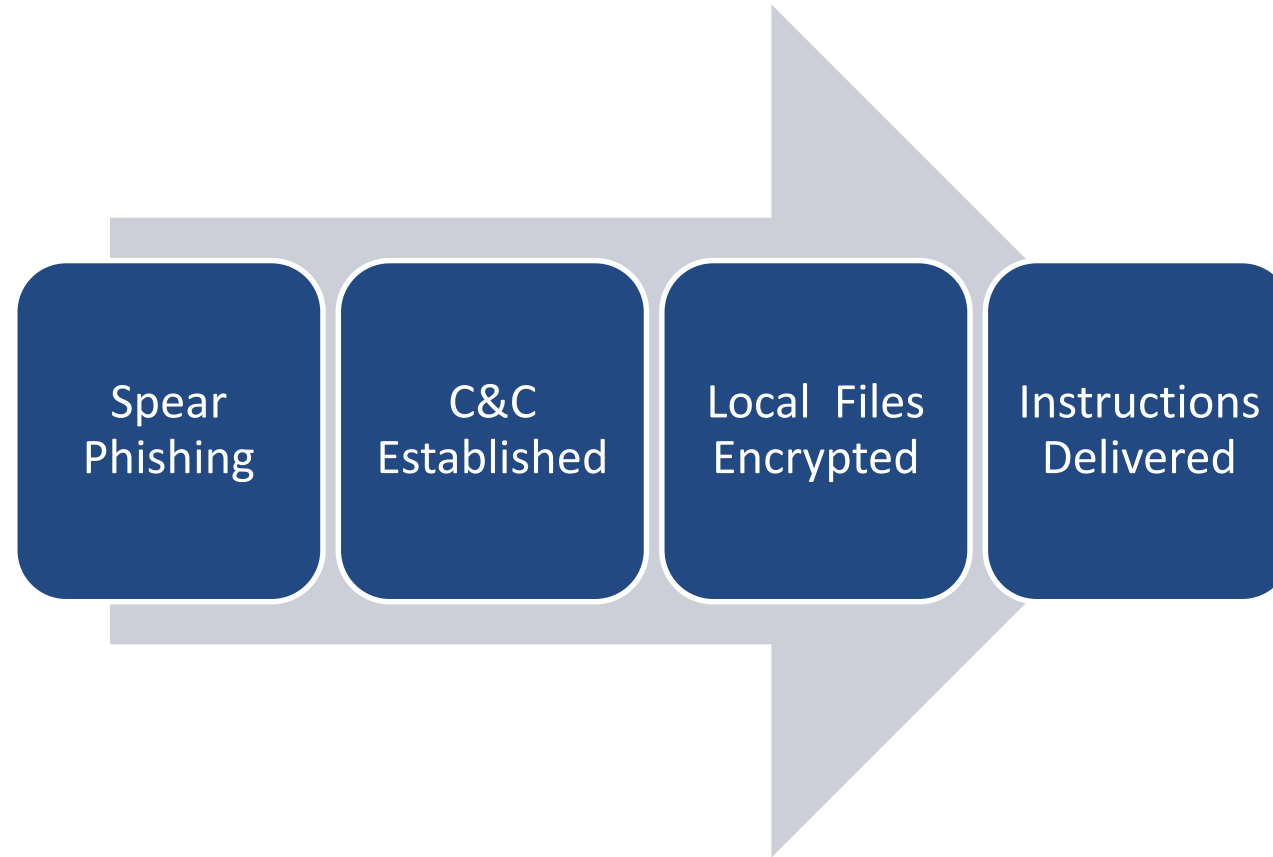
a8wBff-KN4ubE-f2GcKZ-uKZpWW-Z8mbaU-5tXMH5-zjxgZF-yXqHPB-K3z46v-eS6qZt

If you already purchased your key, please enter it below.

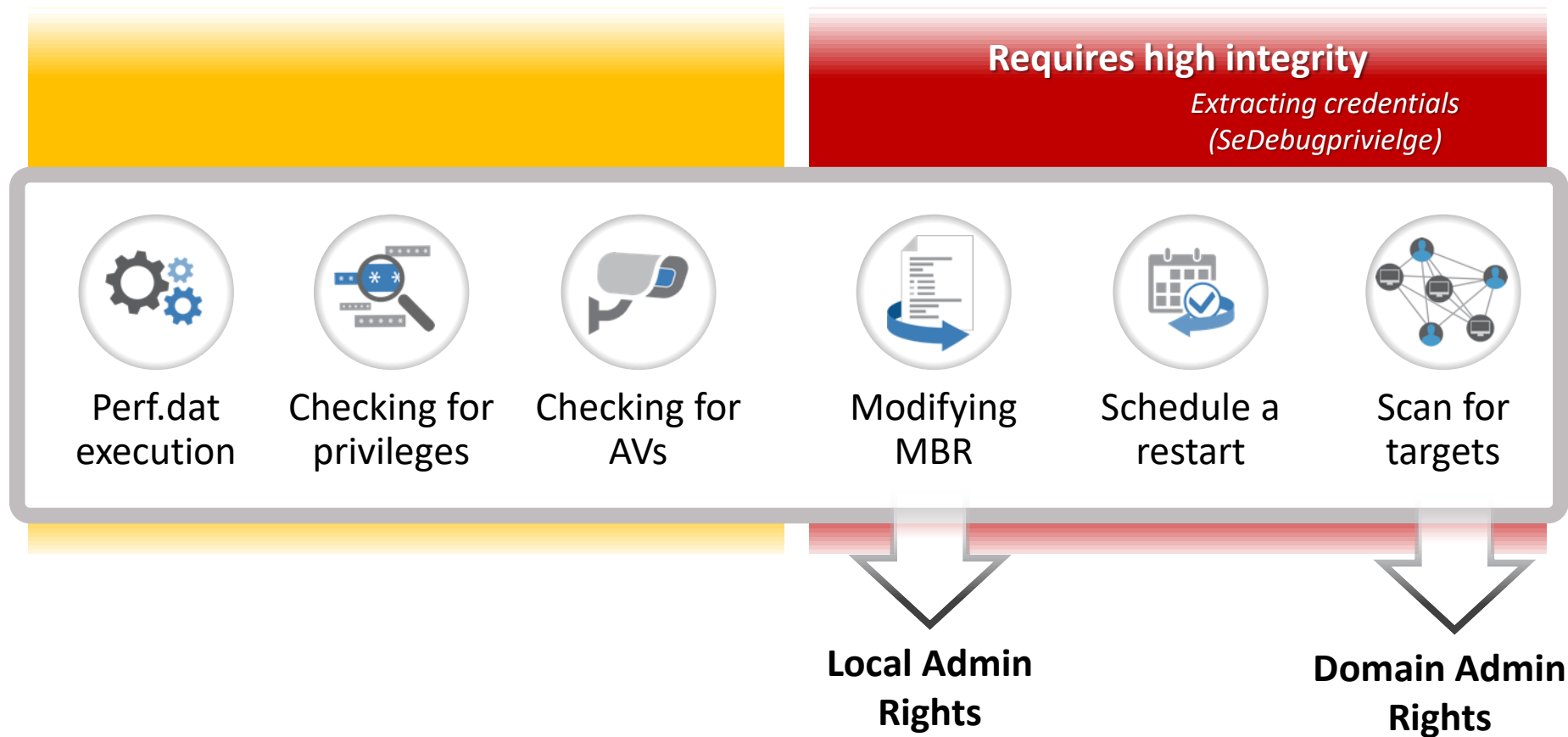
Key:

*Image from ComputerWeekly and bleepingcomputer.com

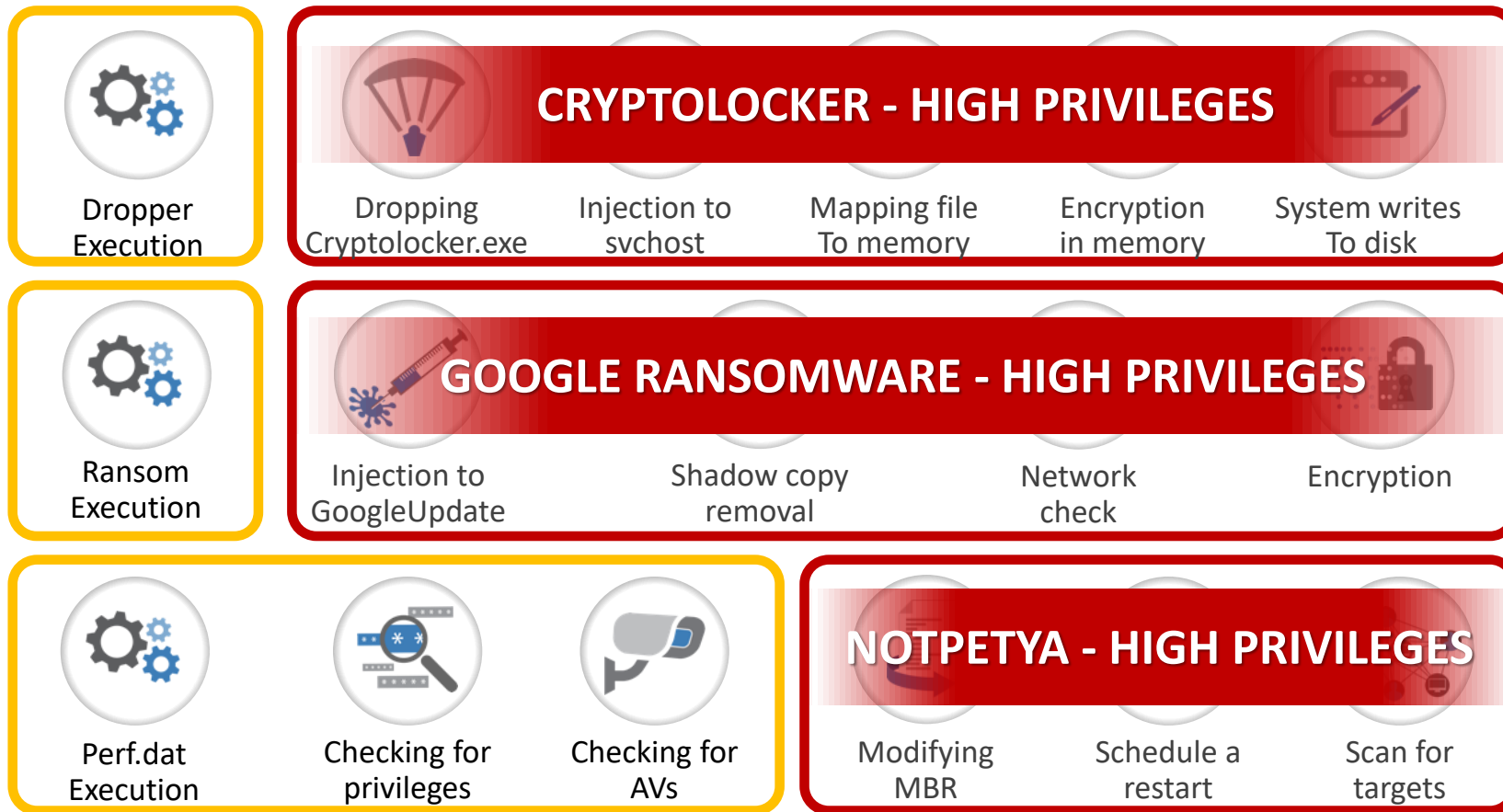
The Opportunistic Ransomware



NotPetya – With Admin Privileges - Kill Chain

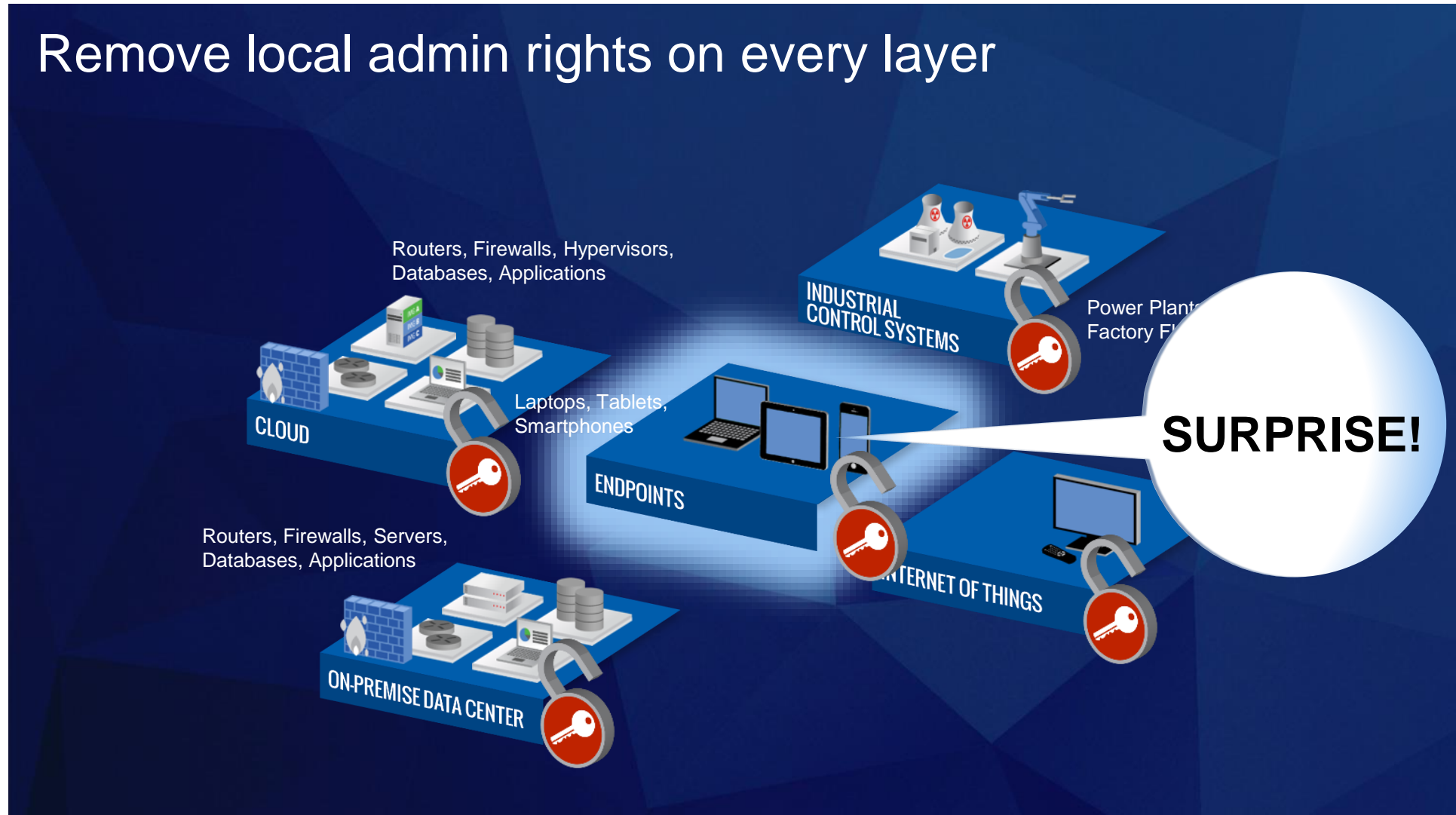


It Really is a Privilege Problem



Recommendation: Implementing Least Privileged Access

Remove local admin rights on every layer



“HOW” TO

APPRECIATE IMPORTANCE OF LEAST PRIVILEGED



“Organizations should exercise the principle of **least privilege for local administrative access**. The vast majority of users do not require local admin access in the modern Windows OS. When an application or service requires administrative privilege, the end user should **log on as a standard user, and privilege should be elevated according to policy**.”

Gartner Technical Professional Advice: Reduce Access to Windows Local Administrator With Endpoint Privilege Management



First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

CIS Controls

- 1: Inventory of Authorized and Unauthorized Device
- 2: Inventory of Authorized and Unauthorized Software
- 3: Secure Configurations for Hardware and Software
- 4: Continuous Vulnerability Assessment and Remediation
- 5: Controlled Use of Administrative Privileges

Best Practice

- Check Company Background/Reputation
 - Verify URL and Company Name in very carefully
 - Contact information
- Personal Data
 - Avoid unnecessary Personal data
 - Understand How the payment work and any third-party payment company involved.
- Endpoint App safety
 - Aware any plug-in or app require to install
 - Avoid any unauthorized App source
- Protect your Endpoint
 - Remove Local Admin Right, login as a Standard user
 - Install Antivirus or any endpoint protection software
 - Deploy Least Privilege Management solution for Corp Users.

THANK YOU !