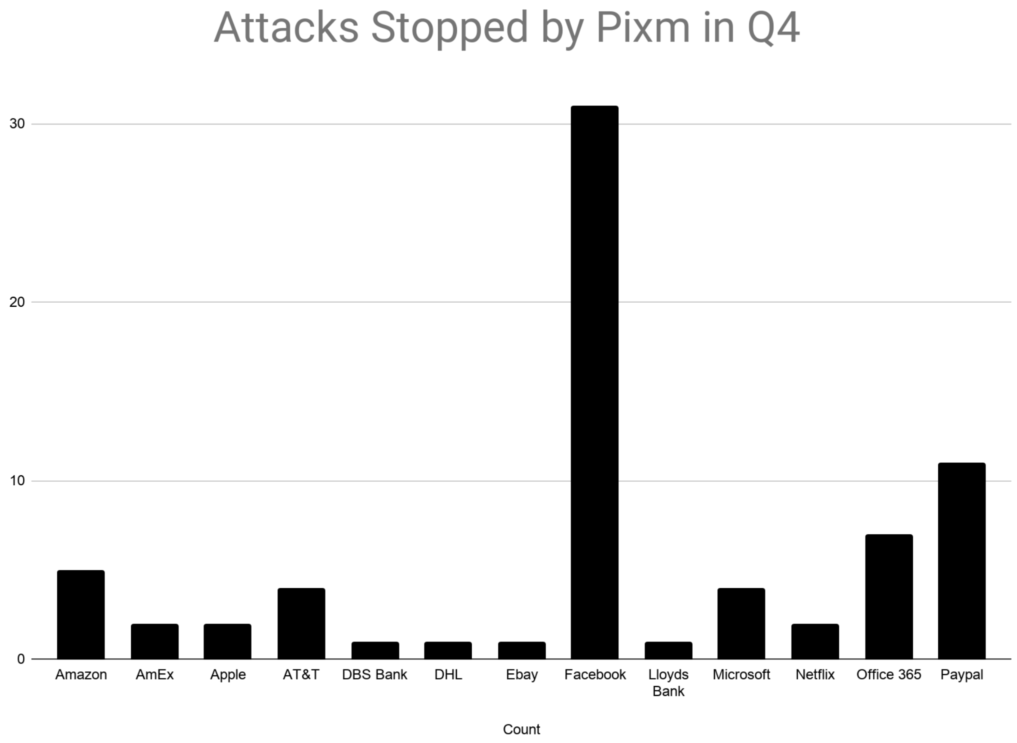
# Consumer Threat Report Q4 2020

After launching our free consumer extension in August of 2020, we grew our user base to 1000 over the following two quarters and stopped over 60 phishing breaches in the final quarter of 2020 alone.

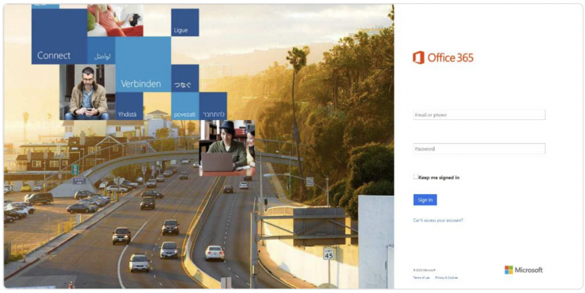
We can see below the breakdown of phishing attacks prevented. These phishing attacks were stopped after end users clicked on actual links. This means that Pixm very likely prevented users from entering their credentials on URLs that bypassed our customer's built in email protection, security products, and browser blacklists like Google Safe Browse.



It's hard to notice the predominant 51% of Facebook phishing attacks.  Many of these were likely delivered on the Facebook platform itself rather than through email. Phishing deliveries like this are entirely outside the scope of corporate security protection. The percentage of sensitive data shared and accessed through non-corporate channels like WhatsApp, LinkedIn and personal email has increased dramatically in 2020. Social media phishing indeed represents an unprecedented risk.

On a related work from home note, 18% of these attacks were on Outlook related applications. For consumers running Pixm on their personal devices, this suggests a worrying amount of work access occurring on non-work devices.

If we observe some of the phishing attacks up close, we see of course the garden variety signin pages impersonating Office 365 and Facebook.

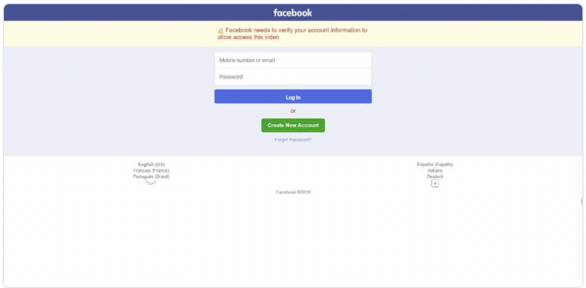


57f94b@anon-user.com

Details ›

https://msupdate.net/landing.php?template_id=cddb68f8-2712-4e7f-aa0a-7134d…

*Opened at 8:59 AM, November 30th*



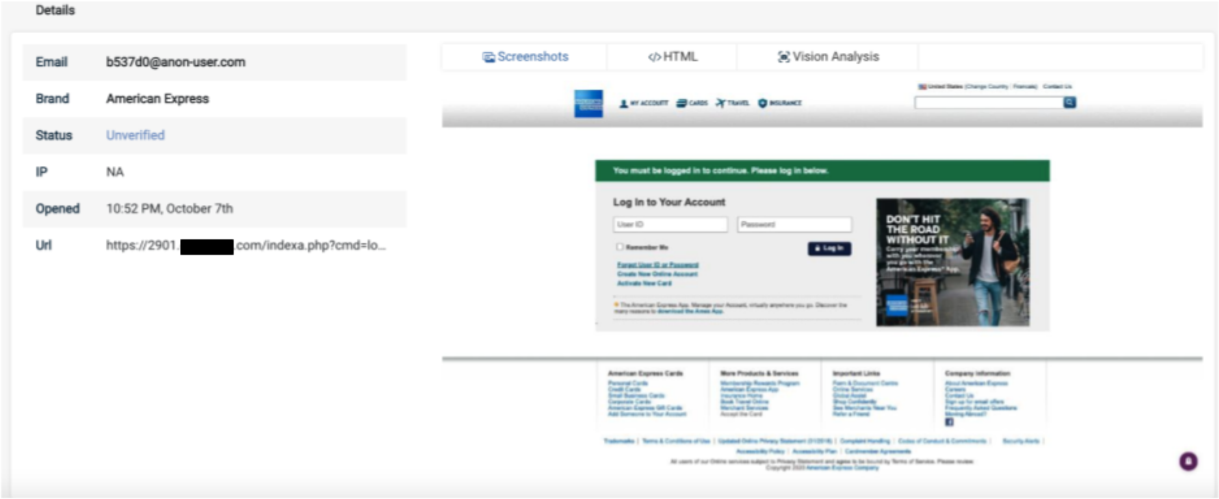
d8ba66@anon-user.com

Details ›

https://jovial-bardeen-fdb26b.netlify.app/

*Opened at 7:36 PM, November 29th*

What allows many of these attacks to evade traditional reputation based security tools is that they are very often hosted on legitimate 3rd party websites that have been compromised. Below we can see an example of an American Express web page hosted on the legitimate domain of a 3rd party accounting education website.



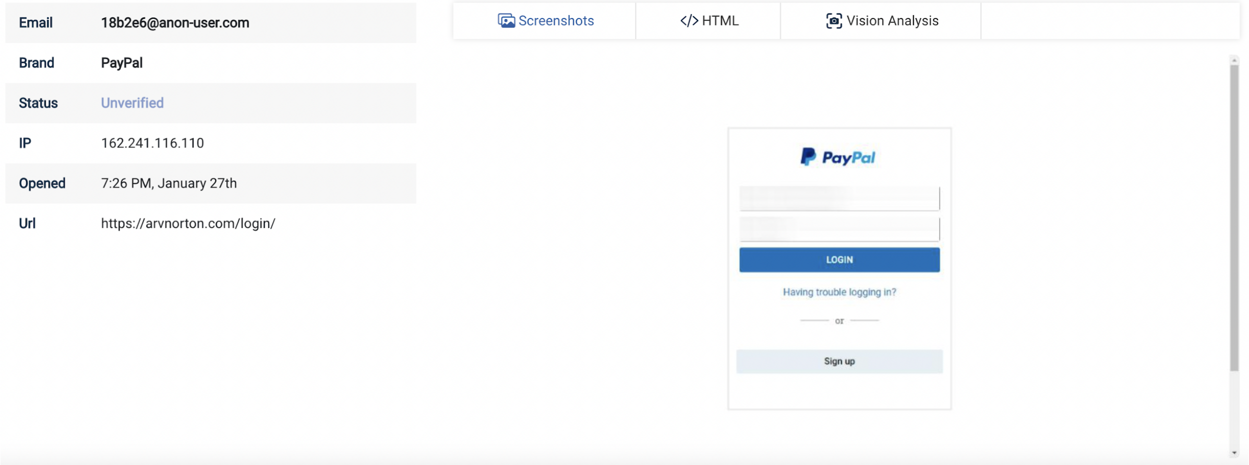
Details

| | |
|---|---|
| Email | b537d0@anon-user.com |
| Brand | American Express |
| Status | Unverified |
| IP | NA |
| Opened | 10:52 PM, October 7th |
| Url | https://2901.[redacted].com/indexa.php?cmd=lo... |

Screenshots
HTML
Vision Analysis
You must be logged in to continue. Please log in below.
Log In to Your Account
User ID
Password
Remember Me
Log In
DON'T HIT THE ROAD WITHOUT IT

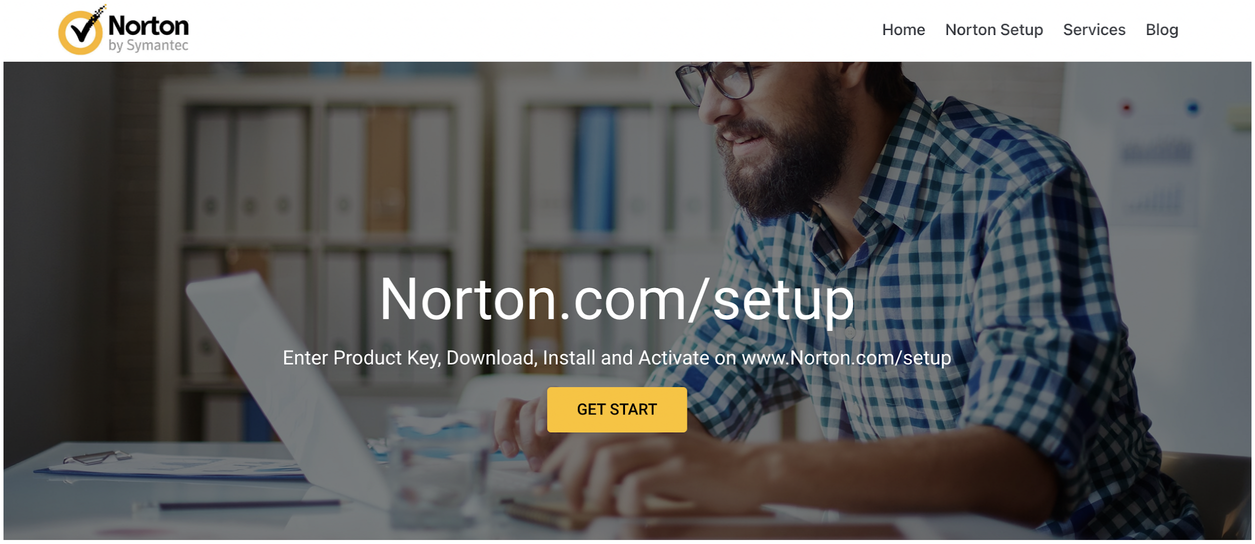
For the privacy of the 3rd party domain, we are not displaying the root domain in the URL. We can observe that the attacker has created a subdomain '2901' to deploy this login page. We've observed dozens of similar cases over the quarter, where hackers breached and hijacked the reputations of online service and small business websites to deliver their attacks undetected.

Another pattern we observed was hackers impersonating security or tech support. Below was a paypal phishing page, whose domain looks very similar to norton.com.



| | |
|---|---|
| Email | 18b2e6@anon-user.com |
| Brand | PayPal |
| Status | Unverified |
| IP | 162.241.116.110 |
| Opened | 7:26 PM, January 27th |
| Url | https://arvnorton.com/login/ |

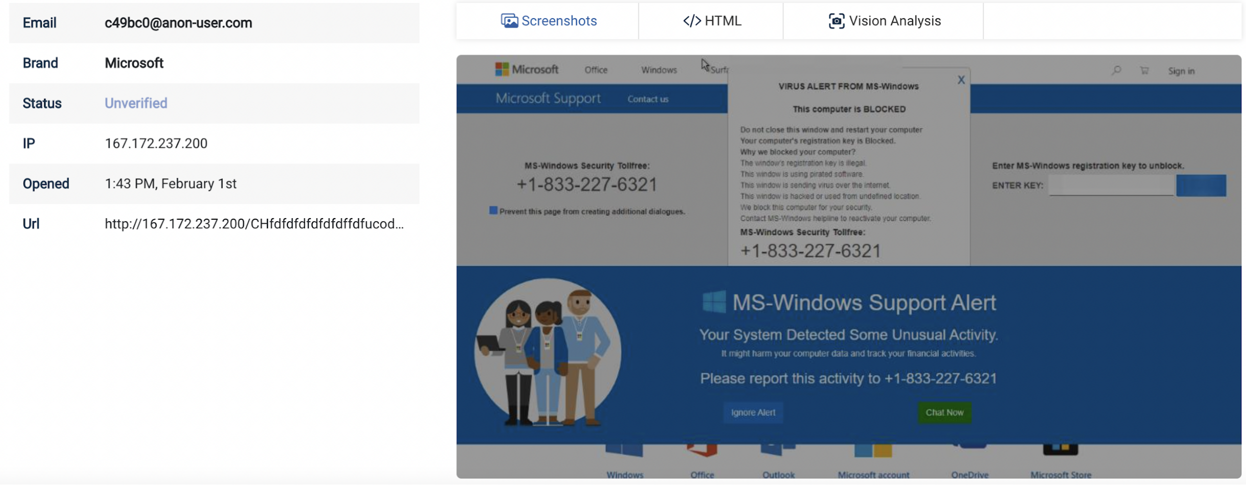
Indeed, opening the domain in an incognito browser leads a user to a Norton security type clone.



Norton.com/setup

Enter Product Key, Download, Install and Activate on www.Norton.com/setup

Even more common was phishing impersonating Windows support alerts, designed to trigger panic and likely to lure users into a vishing scheme.



| | |
|---|---|
| Email | c49bc0@anon-user.com |
| Brand | Microsoft |
| Status | Unverified |
| IP | 167.172.237.200 |
| Opened | 1:43 PM, February 1st |
| Url | http://167.172.237.200/CHfdfdfdfdfdfdffdfucod… |

MS-Windows Security Tollfree:
+1-833-227-6321

Prevent this page from creating additional dialogues.

VIRUS ALERT FROM MS-Windows

This computer is BLOCKED

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?
The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet.
This window is hacked or used from undefined location.
We block this computer for your security.
Contact MS-Windows helpline to reactivate your computer.
MS-Windows Security Tollfree:
+1-833-227-6321

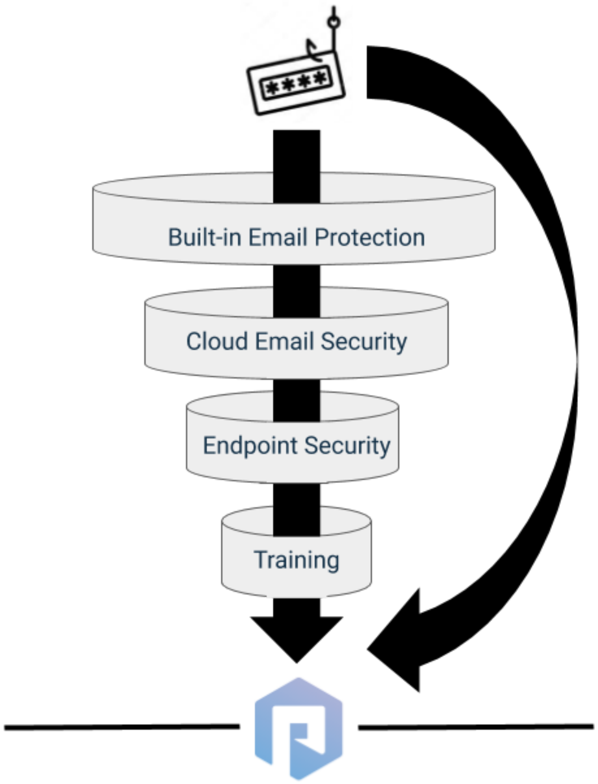
Enter MS-Windows registration key to unblock.
ENTER KEY:

MS-Windows Support Alert

Your System Detected Some Unusual Activity.
It might harm your computer data and track your financial activities.

Please report this activity to +1-833-227-6321

These are just a few methods phishing attacks consistently use to penetrate and entirely flank existing security funnels. Pixm's real time computer vision technology in the browser inserts a final line of defense against phishing attacks.



It is our mission to stop breaches just like these for organizations and deliver the same reporting for insights into phishing vulnerabilities and campaigns that target their users.