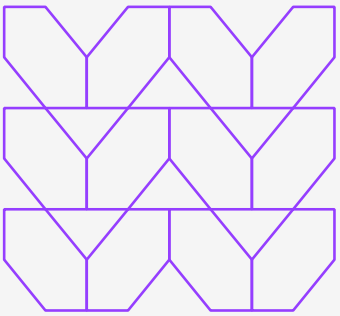
MENLO SECURITY

Decoding a Google Drawings and WhatsApp open redirection phish

The Menlo Security threat research team has uncovered a sophisticated phishing campaign that exploits Google Drawings and the open redirection capabilities of a WhatsApp URL shortener.

Report

Executive **Summary**



Why this is important/interesting:

This attack is noteworthy as it abuses trusted and reputed services like Google and WhatsApp, in what is known as a Living Off Trusted Sites (LOTS) exploit, to host the attack elements used in the kill chain.

Are there IOCs or rules?

Yes. IOCs are available and provided as an addendum to this brief and analysis.

What users can do to protect themselves:

Enterprise users need to look for URL redirection and always check the domain of the link or adopt a tool that provides this protection for their users. Additionally, they need to be wary of new or unknown domains asking the users to enter Amazon login and recovery credentials. Browser security tools can provide such protections automatically.

Threat intelligence

Known threat actor? No

New threat actor? Most likely

Known or new TTPs? Yes. The usage of Google Drawings, WhatsApp URL shortener open redirection, and another URL shortener (qrco[.]de) in the attack kill chain.

Infection vector

Phishing link most likely arrives as an email.

Conclusion

What is your confidence level and assessment of this threat?

The attack appears to be the work of a low-level threat actor who is primarily interested in capturing the user's credentials across a wide blast radius.

What is the probability that this threat gains in activity/popularity?

Based on the analysis, the Menlo Security threat research team assesses with high confidence that the threat actors will continue to create more such phishing attacks using the Google Drawings and WhatsApp URL shortener open redirection.

Decoding a Google Drawings and WhatsApp open redirection phish

With the rapid adoption and established trust in cloud services, threat actors are crafting new ways to host phishing pages in popular cloud applications. A recent discovery highlights how this threat is targeting two of the world's most widely used applications, putting the personal data of billions at risk.

The Menlo Security threat research team has uncovered a sophisticated phishing campaign that exploits Google Drawings and the open redirection capabilities of a WhatsApp URL shortener. This attack combines the reach of Google Workspace, used by over 50% of businesses, and WhatsApp, which has over 3 billion users worldwide, to deceive unsuspecting victims.

Upon further investigation, our threat research team also identified links leading to these sites that abused the open redirection in one of WhatsApp URL shortener services, “l.wl.co,” that redirects to an Amazon phish. The phishing page attempts to harvest sensitive and critical personally identifiable information (PII) like email, password, mother’s maiden name, date of birth, postal address, and credit card details.

While WhatsApp does not have a native URL shortener it does own the domain "l.wl.co," which is often used because the domain was created specifically for shortening URLs for WhatsApp.

This attack demonstrates that the WhatsApp URL shortening service is a versatile tool for cybercriminals, aligning with other findings that financially motivated attackers favor techniques that will give them the most return on investment.

The combination of Google Workspace's vast reach and WhatsApp's global popularity creates a false sense of security for users. This attack is also noteworthy because it abuses trusted and reputed services like Google and WhatsApp, in a classic example of Living Off Trusted Sites (LOTS) to host the attack elements used in the kill chain.

Menlo Security assesses with high confidence that the threat actors will continue to use Google Drawings and WhatsApp URL shortener open redirection for phishing attacks.

This report provides an analysis of the phishing attack kill chain, details the use of open redirection, and provides recommendations for mitigating these attacks.

What is a LOTS attack?

Living Off Trusted Sites (LOTS) is a cyber attack technique that involves using legitimate websites to perform malicious activities without being detected. Threat actors exploit the reputation of trusted sites to carry out their activities, such as hosting phishing pages, operating botnet command and control servers, running dropper sites for malware, and exfiltration.

Potential impact of phishing attacks

This Amazon-themed phish attempts to harvest sensitive and critical personally identifiable information (PII) including email, password, mother's maiden name, date of birth, postal address, and credit card details. Such content is extremely valuable to threat actors, as these credentials do not change often and can be used repeatedly in the following ways:

- The attacker can sell the credentials on the dark web for other threat actors.
- Since email addresses rarely change, victims of this attack may be targeted with similar phishing attempts in the future.
- The attacker can use the harvested credentials to expand the attack if the same information is used on other services and sites including financial or corporate accounts.

Overview

Before diving into the technical analysis, we will provide a general overview and outline of the trusted and reputable services used.

Google Drawings

Google Drawings is diagramming software included as part of the free, web-based Google Docs Editors suite that includes Google Docs, Google Sheets, Google Slides, Google Forms, Google Sites, and Google Keep in Google Workspace. It allows users to create and edit diagrams that can be used to collaborate with others. Unlike many of the other elements of Google Suite, Google Drawings does not have its own dedicated domain. Upon visiting the Google Drawings URL, a new document is created.

Inserting a URL in Google Drawings

One important feature of Google Drawings is that it allows users to insert a link in the page. This can easily be done by selecting the highlighted canvas and inserting the link (see Figure 1).

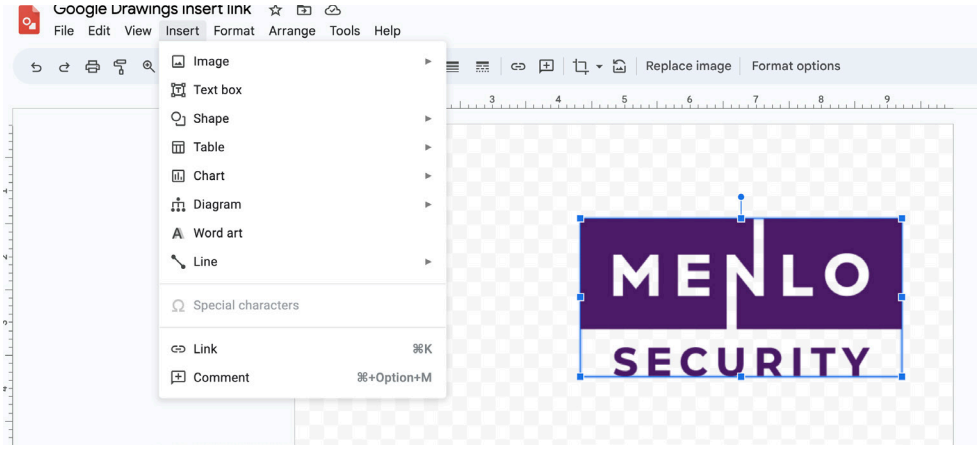


Figure 1: Inserting a link in Google Drawings

If a malicious URL is inserted using this method, it evades traditional security defenses, and appears benign to the victim, thereby increasing the likelihood of clicking the link. With the added collaboration capabilities, the image and the link can also be changed by the attacker without the need to host a new Google Drawings link.

WhatsApp URL shortener service - "l.wl.co"

"l.wl.co" is a URL shortener service that has been owned by WhatsApp since 2010 (see Figure 2).

Whois Lookup

```
Admin City: Menlo Park
Admin City: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Country: US
Admin Email: 03d71b91f97a44efs@fb.com
Admin Organization: REDACTED FOR PRIVACY
Admin Organization: WhatsApp LLC
Admin Postal Code: 94025
Admin Postal Code: REDACTED FOR PRIVACY
Admin State/Province: CA
Admin State/Province: REDACTED FOR PRIVACY
Creation Date: 2010-04-26T07:56:20Z
DNSSEC: unsigned
Domain Name: WL.CO
Domain Name: wl.co
```

Figure 2: "l.wl.co" whois lookup

"l.wl.co" is a subdomain of WhatsApp that redirects to "https://www.whatsapp.com."

"l.wl.co" open redirection

By providing "/l?u=" as a query parameter string and appending a URL, a URL redirection is generated. An example of the URL redirection link to menlosecurity.com is - l.wl.co/l?u=https://www.menlosecurity.com. The packet capture illustrating this activity is shown below (See Figure 3).

Request URL:	https://l.wl.co/l?u=https://www.menlosecurity.com
Request Method:	GET
Status Code:	200 OK
Remote Address:	[2a03:2880:f031:12:face:b00c:0:2]:443
Referrer Policy:	strict-origin-when-cross-origin

▼Query String Parameters view source view URL-encoded

u: https://www.menlosecurity.com

Figure 3: Open redirection example using "l.wl.co"

At the time of this analysis, links created with the WhatsApp URL shortener don't provide any security warnings upon redirection to the user.

A high level depiction of the attack chain of the Amazon-themed phish is shown below (See Figure4).

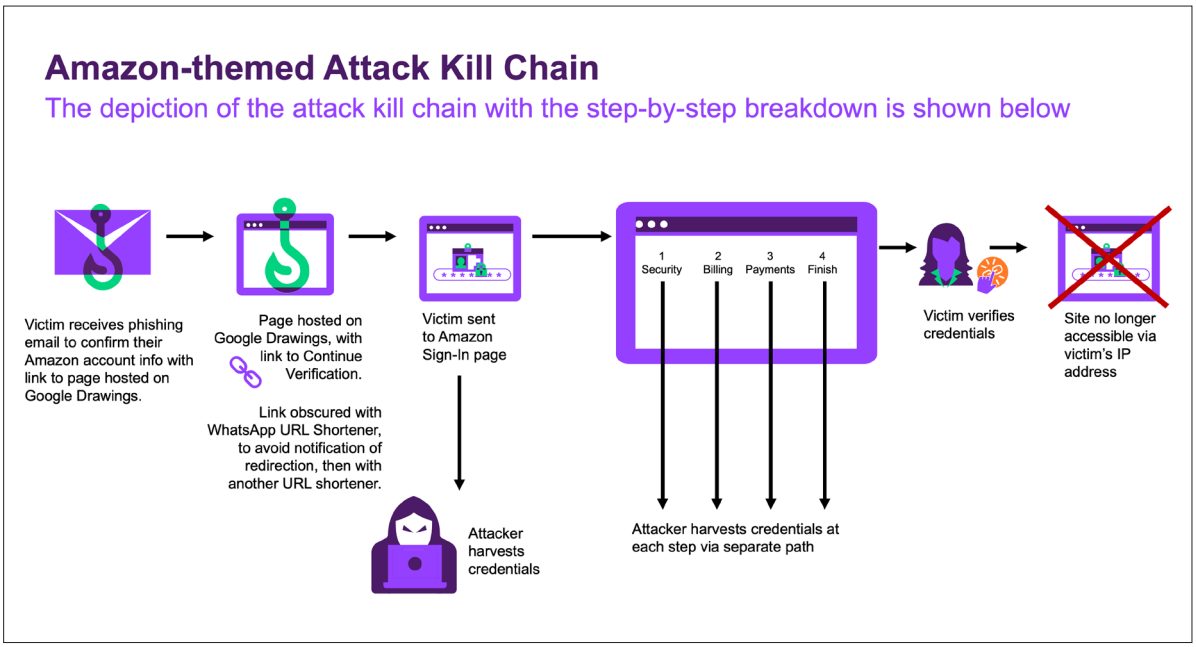


Figure 4: Open redirection example using "l.wl.co"

Analysis of the Amazon-themed phish

Upon visiting one of the phished URLs, at https://docs[.]google[.]com/drawings/d/1ySdWrYp7X3uV4d7cxdQ3-YH7Iw3-el-J0C3bJBaAazw, the victim is presented with an image of the Amazon verification process dialog with a link created using the WhatsApp URL shortener embedded in the Continue Verification button as shown below (See Figure 5).

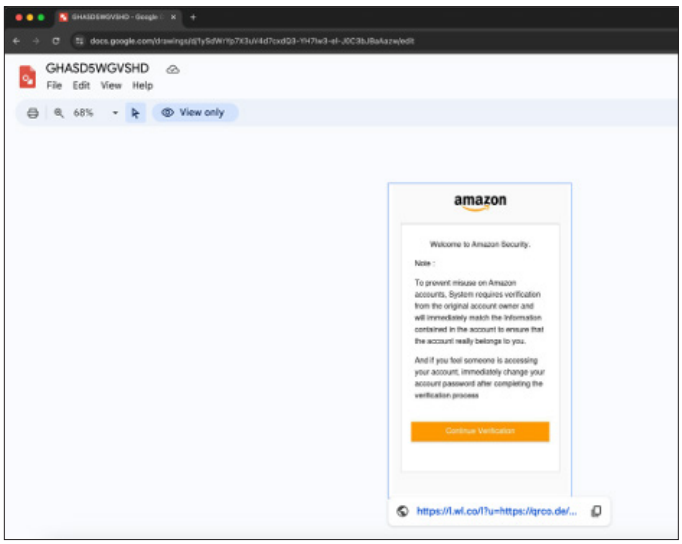
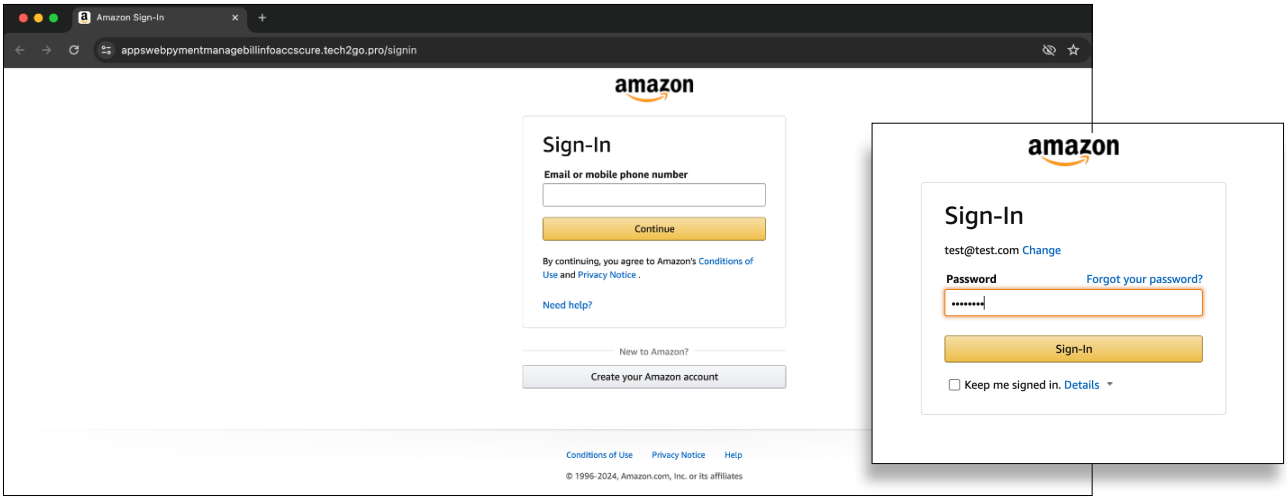


Figure 5: Google Drawings Amazon verification process image

At the time of the analysis, the malicious link embedded in the image was - https://l[.]wl[.]co/l?u=https://qrco[.]de/bfAX9z. Interestingly, the WhatsApp URL shortener is appended with another URL shortener, "qrco[.]de," which is an URL shortener service for dynamic QR codes. We believe that the threat actor used this logic to hide the original link and thereby evade Google URL scanners and possibly others.

The resultant URL from both the URL shorteners, "https[://]appswebpymentmanagebillinfoaccscure[.]tech2go[.]pro/signin" presents a phished Amazon Sign-In page which is followed by a login page after the victim provides their email as shown below (See Figure 6).

Figure 6: Phished Amazon Sign-In and login page



Upon entering the credentials, the victim is presented with four separate login pages, including Security, Billing, Payments, and Finish. All of the credentials are collected using different URL paths hosted in the same domain - /appswebpymentmanagebillinfoaccscure[.]tech2go[.]pro.

The significance of these separate paths is that the victim's information is collected at every stage, rather than only at the end of the process. That means that even if the victim begins to sense that something is "phishy" midway through the sequence, some information has already been harvested.

The details of these pages are as follows:

Security—The phished Security Checkup page asks the victim to provide their mother's maiden name, their date of birth, and phone number as shown below (See Figure 7).

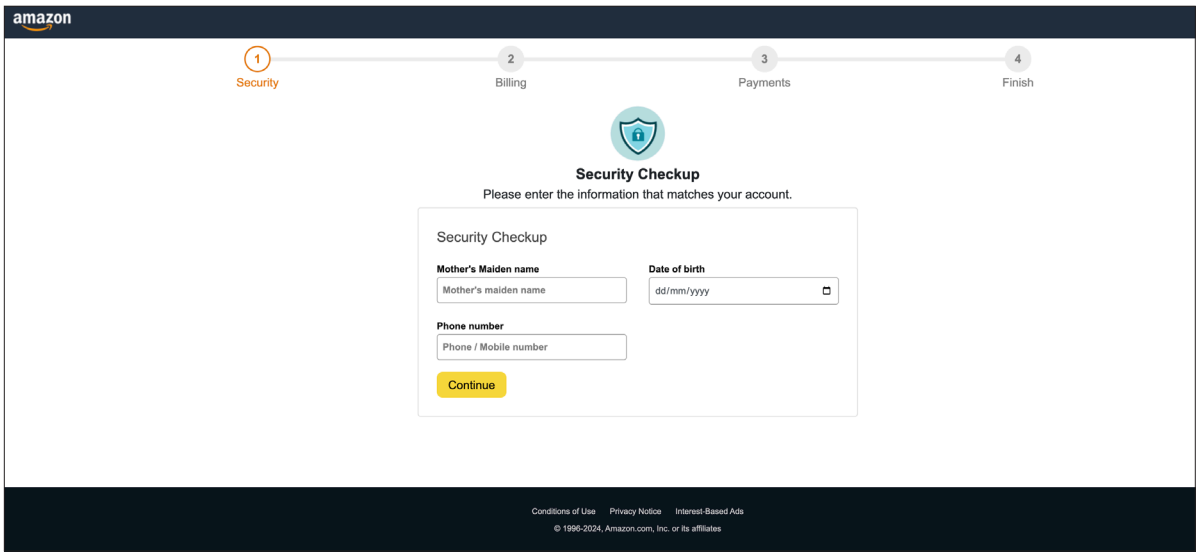


Figure 7: Phished Amazon Security page

Upon entering the details and clicking continue, the phished Billing page is displayed.

Billing—The phished Billing page asks the victim to provide their billing address, including street address, city, state/province/region, and zip code as shown below (See Figure 8).

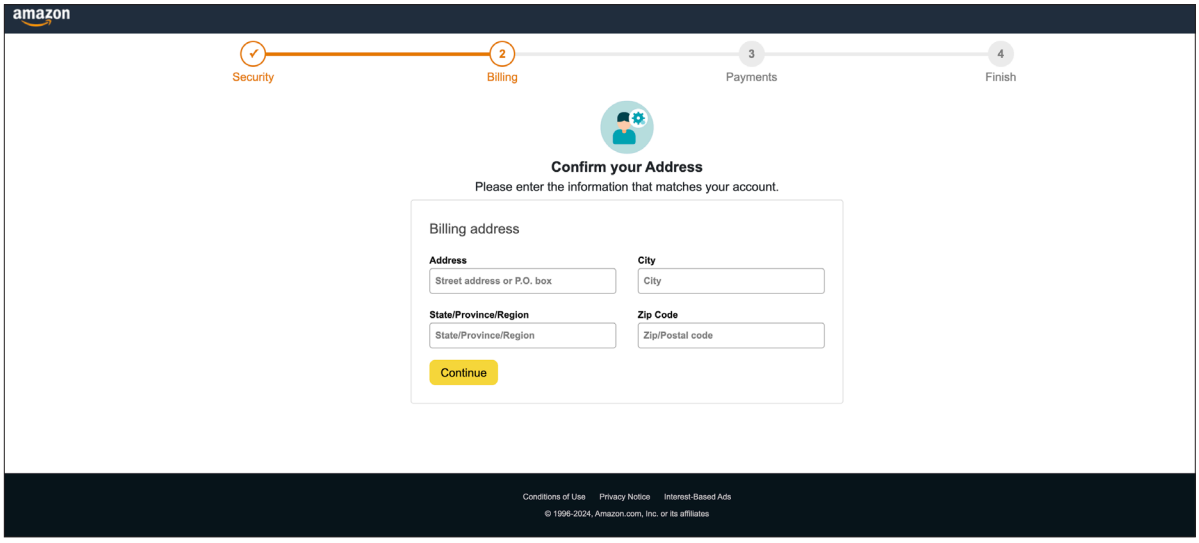


Figure 8: Phished Amazon Billing page

Payments—Upon entering the details and clicking continue, the phished Payments page is displayed. Information requested includes credit or debit card details with the cardholder name, card number, expiration date, and security code as shown below (See Figure 9).

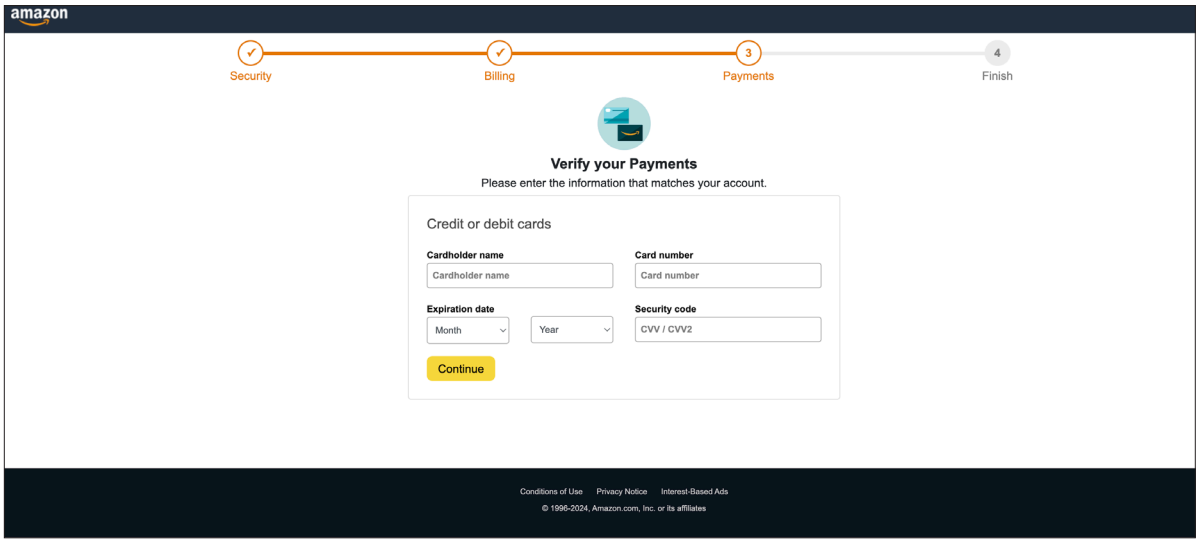


Figure 9: Phished Amazon Payments page

Finish—Upon entering the details and clicking continue, the Finish phished page stating the identity verification is in process, and an account verification email notification is presented to the victim as shown below (See Figure 10).

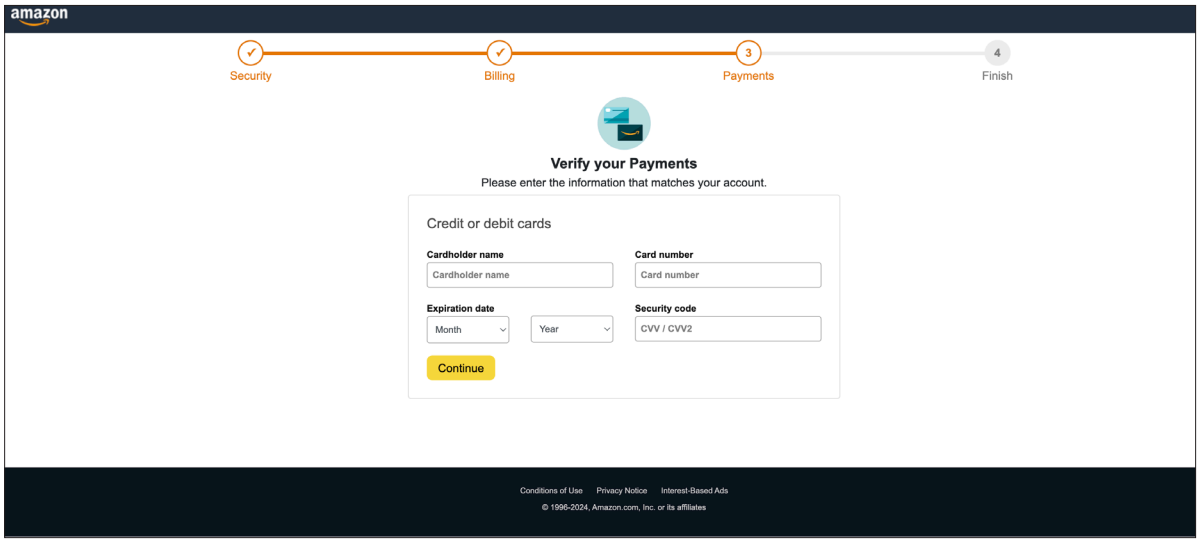


Figure 10: Phished Amazon Payments page

After all these steps, the victim is directed to the original Amazon login page. The attacker then includes additional checks and conditions that mirror what an authentic secure site would request, including:

- Validating the username format and password length.
- Validating credit/debit proper card format.

Once the credentials in the phished page have been entered and validated, the webpage is no longer accessible from the victim's IP address, effectively covering the attackers' trail.

Menlo Security Stance—HEAT Shield

Menlo Security HEAT Shield protects users against such zero-hour phishing attacks using real-time online protection and AI-based analysis. HEAT Shield uses unique AI-powered technology that combines proprietary computer vision, dynamic risk scoring, an object detection model, and analysis of web page elements to analyze dynamic web content. The combination of these factors performs detection in real time with high accuracy for immediate response and protection for users.

This provides users a robust solution in detecting phishing websites even if the attacker takes the following steps to hide their actions:

- Changes the URL of the phishing websites and hosts them in a new infrastructure.
- Dynamically changes the logo of the phishing website.

Customers who are using HEAT Shield are protected against this open redirect Amazon-themed phish. Upon visiting the URL, HEAT Shield blocks the page and categorizes the brand, thereby labeling the page as Phishing (see Figure 11).

Figure 11: HEAT Shield detection of the Amazon-themed phish

Conclusion

Our research and discovery of these phishing attacks reveals an alarming trend: attackers are seeking ways to evade security measures by abusing trusted services. This phishing campaign, utilizing Google Drawings, WhatsApp URL shortener's open redirection, and a second URL shortener, “qrco[.]de” in the attack kill chain is a classic example.

While we have seen Amazon-themed phishing links hosted in Google Drawings in the past, it is highly likely that there are other such phished links impersonating popular brands using different URLs. At this juncture, traditional security defenses that rely on URL categorization fail to provide a comprehensive detection.

Menlo Security HEAT Shield, with its cutting-edge AI-powered technology, combined with computer vision, dynamic risk scoring, object detection model, and analysis of web page elements, provides the ideal solution for detecting these zero-hour phishing attacks.

Menlo Security Browsing Forensics provides even more protection. When configured to capture user sessions if a highly evasive and adaptive threat (HEAT) event is detected, SOC and security teams can see the actual screens that the user visited, along with user inputs. Browsing Forensics also captures page resources, including JavaScript, CSS, HTML, and more, which gives threat hunters an opportunity to analyze the methodology of the attack even if the page itself is no longer live.

To learn more about new threats uncovered by the Menlo Security threat research team, read our recent Global Cyber Gangs Threat Report.

Indicators Of Compromise (IOC)

https://docs[.]google[.]com/drawings/d/1ySdWrYp7X3uV4d7cxdQ3-YH7Iw3-el-J0C3bJBaAazw
https://l[.]wl.co/l?u=https://qrco[.]de/bfAX9z
https://appswebpymentmanagebillinfoaccscure[.]tech2go[.]pro

MENLO SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.