

Blue Team Level 1 Certification
(Standard)

Introduction to BT1

 Welcome to Blue Team Level 1!

4 Topics

 Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

 Introduction to Security Fundamentals

1 Topic

 Soft Skills

7 Topics

 Security Controls

5 Topics 1 Quiz

 Networking 101

6 Topics 1 Quiz

 Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

 PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

 PA2) Types of Phishing Emails

10 Topics 2 Quizzes

 Section Introduction: Phishing Emails Reconnaissance Spam False Positives Credential Harvester Social Engineering Vishing, Smishing Whaling Malicious Files [Video] Types of Phishing Attacks & Examples Lab) Categorizing Phishing Emails Activity) End of Section Review: Phishing Emails PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

 PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

 PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

 PA6) Taking Defensive Actions

12 Topics 1 Quiz

 PA7) Report Writing

7 Topics 1 Quiz

 PA8) Phishing Response Challenge

3 Topics 1 Quiz

Credential Harvester

Blue Team Level 1 Certification (Standard) > PA2) Types of Phishing Emails > Credential Harvester

COMPLETE



Credential harvesters are arguably the most common phishing emails out there, because they are targeting human weaknesses to attempt to retrieve valid credentials which can potentially be used to gain access to numerous services and accounts as a result of credential stuffing attacks.

These emails typically feature a lure email that is styled to look like it is from a legitimate company, impersonating some of the most popular online services and retailers such as Outlook, Amazon, and DHL. The email will tell the recipient to click a button or URL, where they will typically be presented with a real-looking login portal – however, any credentials entered are either stored on the site in an inaccessible directory, or emailed to a dummy account, typically utilizing free online mail services such as Gmail, Hotmail, and Outlook, where the attacker can log in and collect them.

It is important that you feel comfortable with identifying credential harvesters, as they can be very damaging if users enter in their details, potentially compromising their work accounts, personal accounts, and opening themselves up to further attacks such as fraud, social engineering, business email compromise, or blackmail.

Credentials harvesters are sometimes tailored to impersonate login portals for the organization that is being targeted, increasing the chance that employees will fall for it, and enter credentials that they use for work accounts. Logos and other branding material can often easily be retrieved from a company's website, or search engine results.

AMAZON HARVESTER

Real-world Amazon harvester previously active at [hxps://amazonupdates.systes\[.\]net/ap/signin?](http://hxps://amazonupdates.systes[.]net/ap/signin?)

Email Element

**Hello,**

Your Amazon Prime membership is set to renew on May, 5 2020 GMT. However, we've noticed that the card associated with your Prime membership will expire before your renewal date. Please [click here](#) to log-in to your account and update your default payment method information.

To prevent interruption of your benefits, we will try charging other active cards associated with your Amazon account if we can't charge your default card. If we are still unable to process the charge for your membership fee, your Amazon Prime benefits will be paused. If you have any questions and wish to contact us, [click here](#).

Thank you,

The Amazon Prime Team

Update Payment Information

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics | 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics | 1 Quiz

TI4) Tactical Threat Intelligence

7 Topics | 2 Quizzes

TI5) Strategic Threat Intelligence

5 Topics | 1 Quiz

TI6) Malware and Global Campaigns

6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics | 5 Quizzes

DF3) Digital Evidence Collection

8 Topics | 1 Quiz

DF4) Windows Investigations

3 Topics | 3 Quizzes

DF5) Linux Investigations

4 Topics | 2 Quizzes

DF6) Volatility

3 Topics | 1 Quiz

DF7) Autopsy

4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics | 1 Quiz

SI2) Logging

6 Topics | 2 Quizzes

SI3) Aggregation

2 Topics | 1 Quiz

SI4) Correlation

6 Topics | 1 Quiz

SI5) Using Splunk

5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics | 1 Quiz

IR2) Preparation Phase

10 Topics | 3 Quizzes

IR3) Detection and Analysis Phase

7 Topics | 5 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics | 1 Quiz

Your membership has a monthly duration and will be extended automatically for £7.99/month. If you don't want your membership to extend automatically, you may change this in Your Account at any time by selecting "end membership" and you won't be charged for the next membership period. You can always request a refund of your most recent membership fee if neither you nor anyone authorised by you to use your account has taken advantage of any Prime benefits in that membership period.

For any complaints or queries, please contact [Customer Services](#).

For further information about Prime, please refer to the [Amazon Prime Terms and Conditions](#).

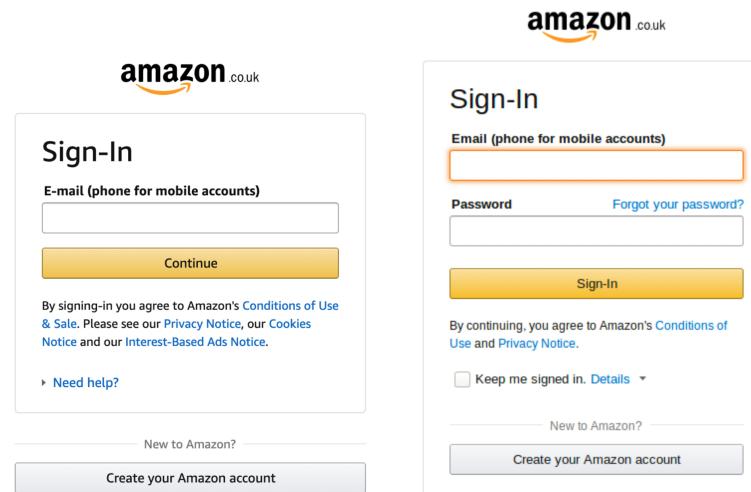
For customers who live outside the UK, [learn more here](#) about what Prime has to offer.

Amazon.co.uk is a trading name for Amazon.

Please note: this message was sent from a notification-only address that can't accept incoming messages. Please do not reply to this message. If you have any questions and wish to contact us, [click here](#).

Web Element

This credential harvester has very effective styling and looks like the real Amazon login page. We have placed images of both side-by-side – can you tell which one is the real Amazon login portal, and which is the malicious one?

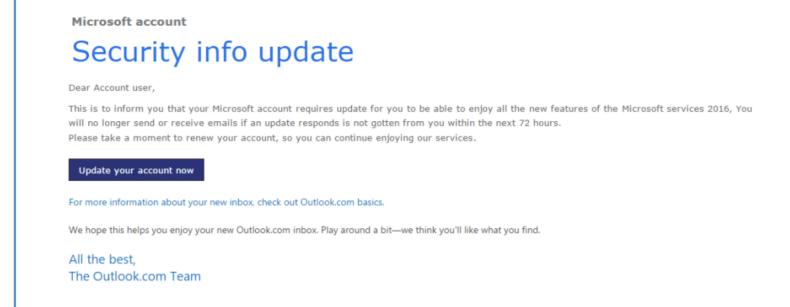


If you said the first image is fake, then you'd be right. Sometimes it's not easy to tell, and you can see why people can fall victim to this type of phishing attack. The main giveaway is typically the URL – if it's not Amazon.com, then it's not Amazon! In this case, the URL is actually very effective, due to a tactic called "sub-domain impersonation" which we will cover in the next section of this domain, PA3) Tactics and Techniques Used.

MICROSOFT HARVESTER

Real-world OWA harvester previously active at [hxps://12.158.186\[.\]j80/owa/auth/logon.aspx](http://hxps://12.158.186[.]j80/owa/auth/logon.aspx)

Email Element



Web Element

This credential harvester is imitating Outlook Web Access, and is very clean and simple. The most notable part of this campaign is that the URL in the email is using an IP address instead of a domain name (such as Google.com). This should immediately generate red flags and be treated as suspicious.

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

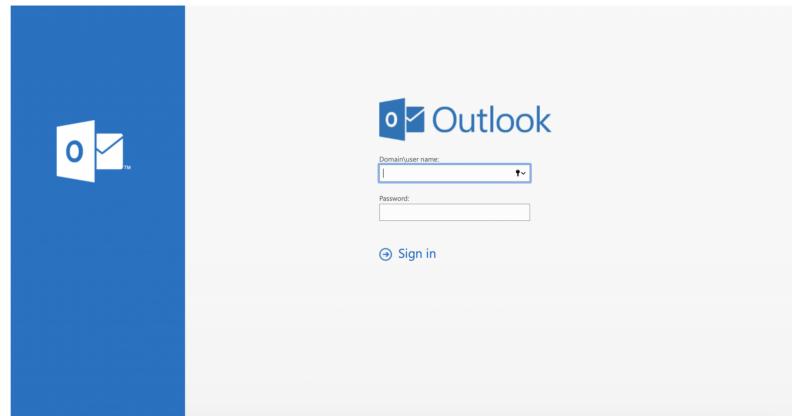
13 Topics | 2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam



KEY POINTS

Below is a list of key points that often apply to credential harvester emails.

- Imitates commonly-used websites and services (such as Outlook, Amazon, HMRC, DHL, FedEx, and many more).
- Entices the recipient to enter credentials into a fake login portal.
- Uses social-engineering tactics including; creating a sense of urgency, and using false authority.
- URLs may be completely random or attempt to copy the legitimate domain name of the organization they are masquerading as.
- Often have small spelling or styling mistakes, something that is extremely rare with legitimate emails coming from big brands and organizations.

[Previous Topic <](#)

[Back to Lesson](#)

[Next Topic >](#)

[Privacy & Cookies Policy](#)

