Credential Harvester

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.

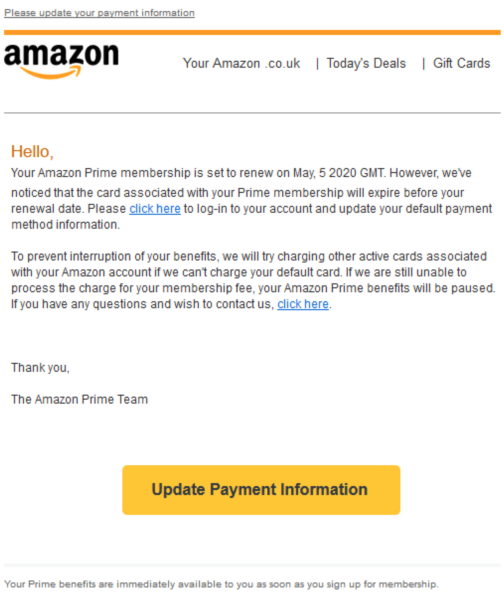
It is important that you feel comfortable with identifying credential harvesters, as they can be very damaging if users enter in their details, potentially compromising their work accounts, personal accounts, and opening themselves up to further attacks such as fraud, social engineering, business email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

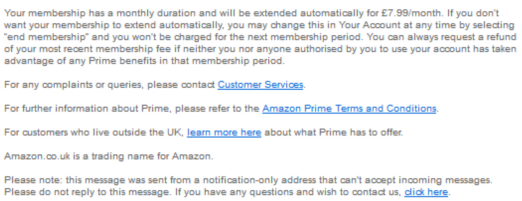
Credentials harvesters are sometimes tailored to impersonate login portals for the organization that is being targeted, increasing the chance that employees will fall for it, and enter credentials that they use for work accounts. Logos and other branding material can often easily be retrieved from a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

AMAZON HARVESTER

Real-world Amazon harvester previously active at hxxps://amazonupdates.sytes[.]net/ap/signin?

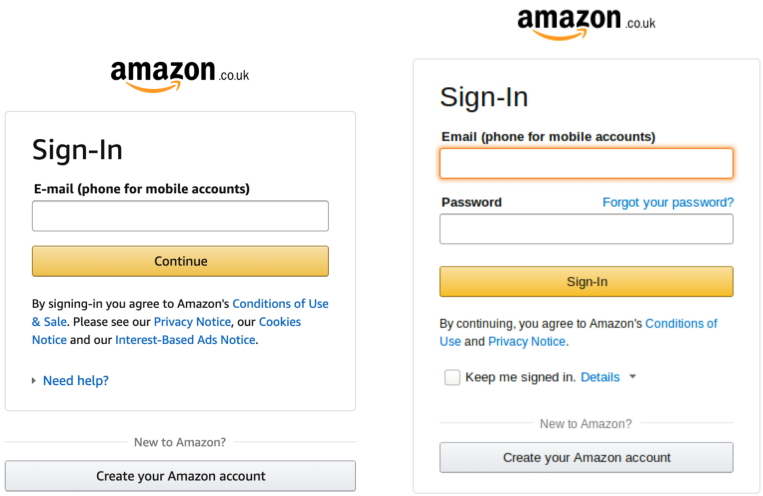
Email Element





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?

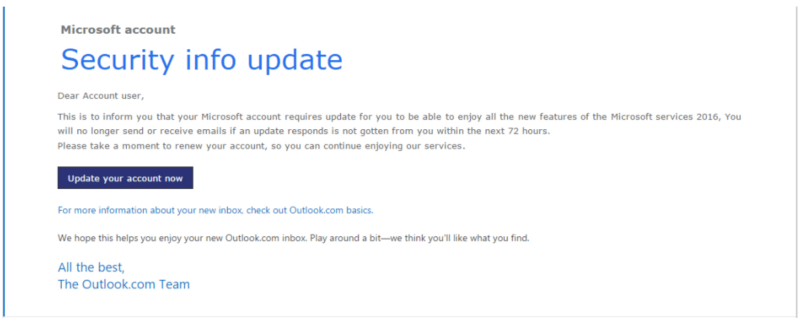


If you said the first image is fake, then you'd be right. Sometimes it's not easy to tell, and you can see why people can fall victim to this type of phishing attack. The main giveaway is typically the URL – if it's not Amazon.com, then it's not Amazon! In this case, the URL is actually very effective, 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

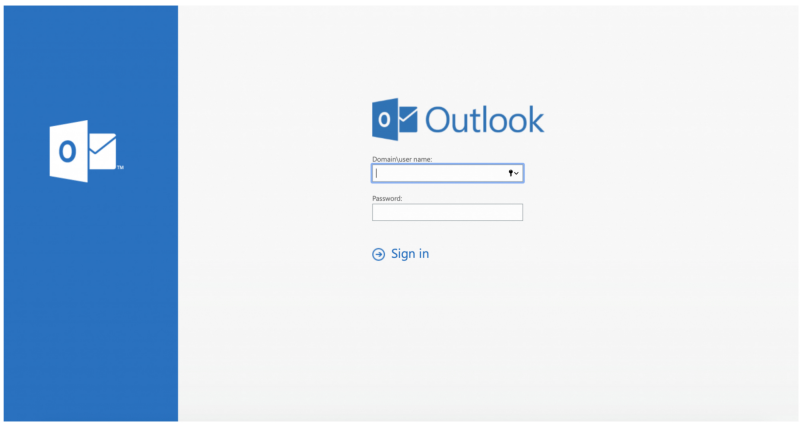
Real-world OWA harvester previously active at hxxps://12.158.186[.]80/owa/auth/logon.aspx

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.



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