

#NoFilter: Exposing the Tactics of Instagram Account Hackers

 [trendmicro.com/en_us/research/21/g/no-filter--exposing-the-tactics-of-instagram-account-hackers.html](https://www.trendmicro.com/en_us/research/21/g/no-filter--exposing-the-tactics-of-instagram-account-hackers.html)

July 12, 2021

Cyber Threats

What tactics do Instagram account hackers use? What do these cybercriminals do with stolen accounts? How can users protect their accounts? We look into Instagram account hacking incidents from a security researcher's perspective and share recommendations for users of Instagram and other social media platforms.

By: Jindrich Karasek July 12, 2021 Read time: 7 min (1898 words)

Updated July 19, 2021: Added information on Instagram's new Security Checkup feature.

Numerous people use social networking sites such as Facebook, Twitter, and Instagram for both personal and business purposes. Instagram alone has over a billion users every month — roughly an eighth of the world's current population.

And like bees to nectar, cybercriminals also flock to these popular sites as they hunt for hacking and extortion prey. In recent years, we have observed various groups and baits linked to such schemes.

In this article, we examine another Instagram account hacking campaign carried out by individual actors or by hacking groups. For maximum impact, the hackers behind this campaign hound social media influencers, a pattern that has also been seen in past campaigns. Having amassed thousands, if not millions, of followers and often earning from brand deals, affiliate marketing, and other means, influencers have so much to lose should their accounts get compromised.

Why is it important to investigate such a campaign? As the adage goes, “Knowing is half the battle,” and the same can be said of this scheme. A heightened awareness of the tactics used in the campaign means fewer people will be fooled into practically handing over their account credentials to cybercriminals. Also, examining this and other, similar schemes reminds users to never take proper cybersecurity hygiene for granted.

How cybercriminals hack Instagram accounts

To bait targets, hackers often disguise their accounts as technical support accounts. Sometimes, they assume the identity of a friend of the target account owner.

They then use phishing emails, messaging apps such as Telegram and WhatsApp, or Instagram itself to reach out to the potential victim. They either create new accounts or reuse stolen accounts for this purpose. Their initial message doesn't address the account owner by name. Instead, the message opens with a generic greeting, which is one of the telltale signs of a scam.

As in a campaign we observed in the past, the content of the hackers' messages claims either that the account owner has committed a copyright violation or that they can provide a verified badge. According to the hackers' message, the account will be deleted if the user will not verify their account by entering their information in a webpage to which a link is included by the hackers in the message. The link leads to a phishing site that mimics the official Instagram user interface.

Hello, Dear Instagram User!

As the Instagram team, we have recently reviewed your account on complaints received by us and realized that you have violated our copyrights, we send you a warning message due to the problems this may cause.

Your Instagram account will be permanently deleted from our servers within 24 hours as you violate our copyrights, if you think this is an error, you can appeal, you can send us your account with the appeal form we will give you, otherwise your account will be closed within 24 hours.

Figure 1. A message from the hackers to a target account owner

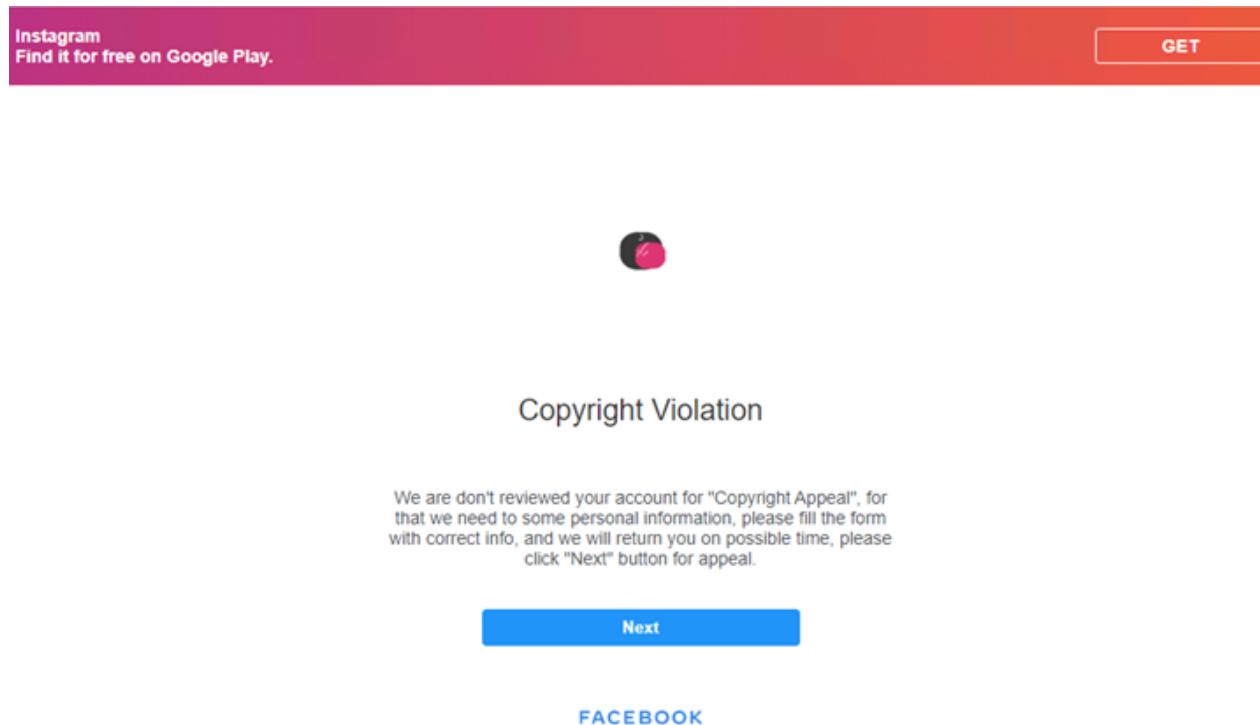


Figure 2. A phishing page claiming that the target account owner has committed a copyright violation

After selecting “Next” in the phishing page, the user is asked to enter the username of the account in question. It should be noted that the phishing site does not verify whether the username indeed belongs to a valid Instagram account.

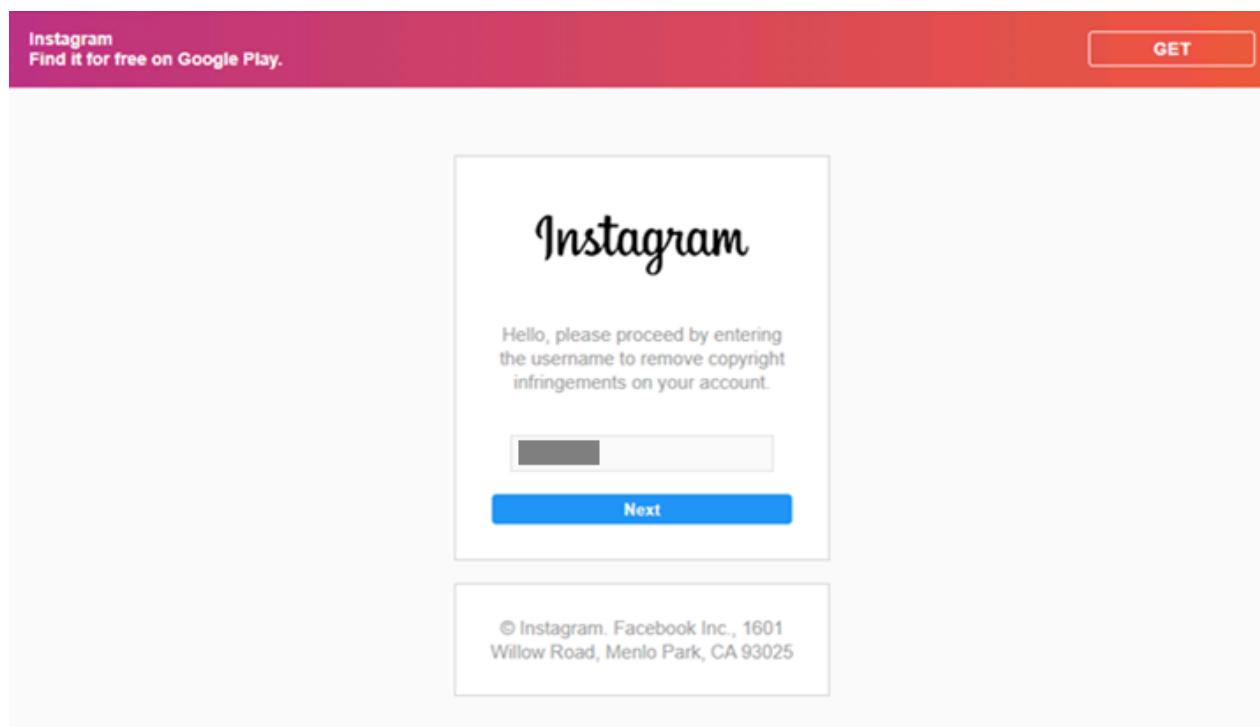


Figure 3. A phishing page requesting the target account owner’s username

The user is then asked to enter the password for the Instagram account, the email address associated with the account, and the password for the email address. Again, the phishing site accepts even invalid and incorrect credentials. The “Continue with

Facebook” button also does not work.

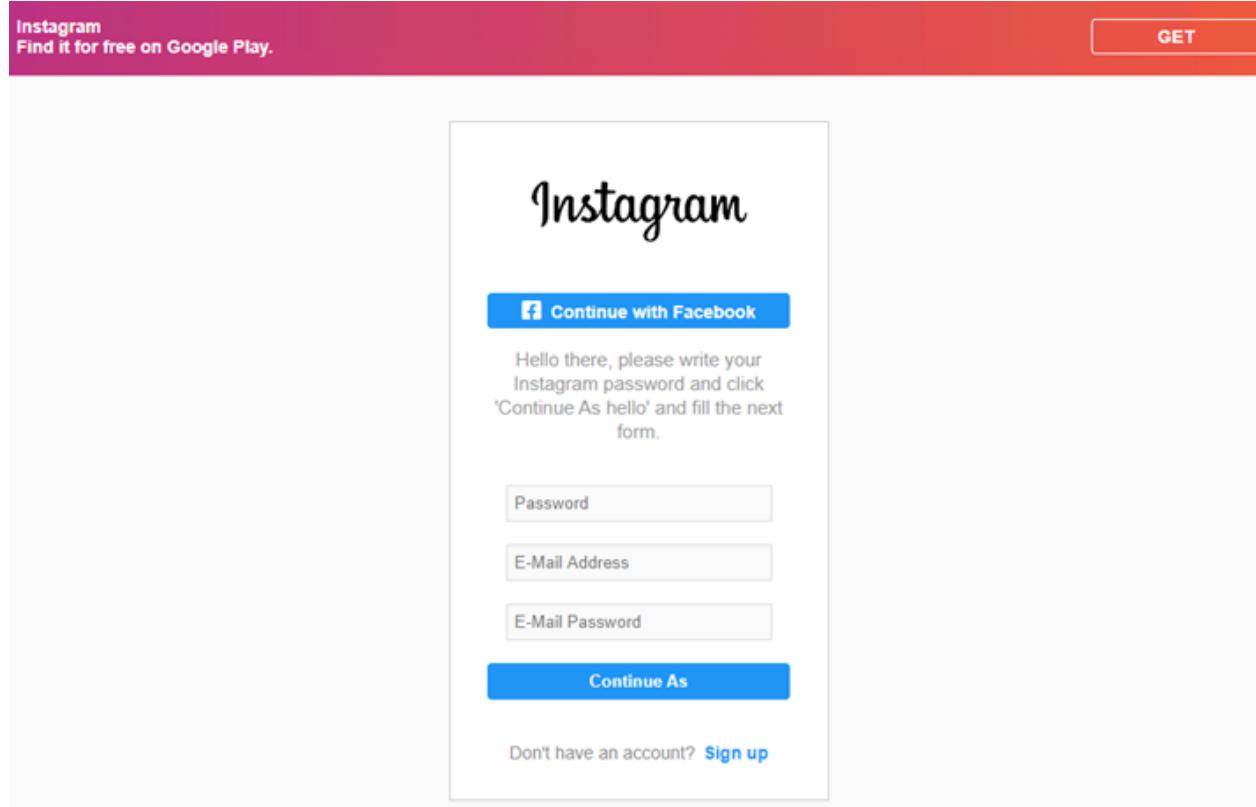


Figure 4. A phishing page requesting the target account owner’s password, email address, and email password

After the user selects “Continue As,” the site shows a confirmation page. The page also instructs the user to not change their account information, ostensibly to give the hackers sufficient time for the withdrawal of the copyright infringement claim. But actually this message is included by the hackers so that they can buy enough time for logging in to the account using the credentials provided by the user.

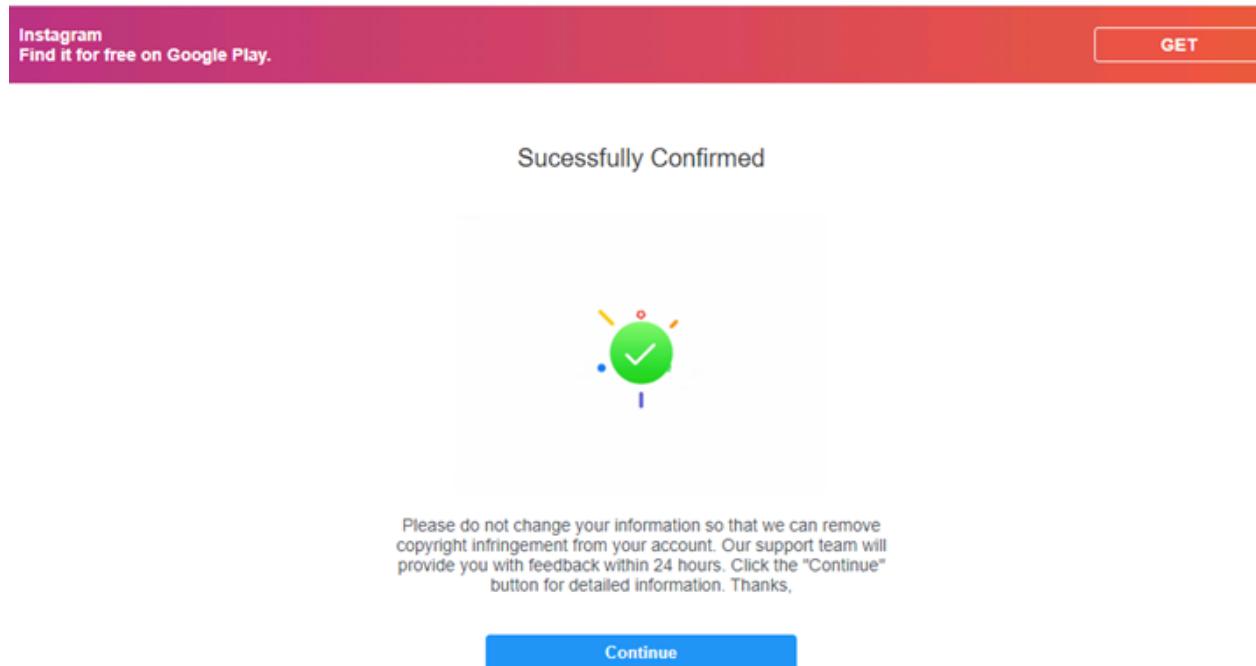


Figure 5. A phishing page showing a confirmation message after the target account owner enters the requested credentials

Selecting “Continue” in the confirmation page leads to the section on copyright on the actual Instagram support site. This is included by the hackers in the phishing site supposedly in a bid to lend some credence to their scheme.

Figure 6. The section on copyright on the actual Instagram support site, to which the phishing site’s confirmation page leads

If the user unwittingly hands over their real credentials, the cybercriminals proceed to change the account’s password so that the original owner loses access to the account. They then mine the account by downloading all images and messages either manually or

through Instagram's data backup feature. The hackers might even modify the account bio, share content via the stories feature, or reach out to the victim's contacts.

At the same time, the hackers start to negotiate with the victim. They usually operate the hacked account while the victim talks with them using a different account. They then demand payment in the form of bitcoin, prepaid credit cards, or vouchers in exchange for the restoration of access. Based on the activity spotted in some of the bitcoin wallets related to this campaign, it seems that some targets might have paid up.

However, the negotiation is merely a ruse. They do this only so that the victim will not be compelled to report the incident via the proper channels, and so that they can buy some time, as downloading all the data from the account can take up to two days. After the victim pays up, the hackers will not give back the account. On the contrary, they will just ask for more payment.

On many occasions, a single malicious actor is manually compromising several accounts at once. There are also cases where each malicious actor belonging to a group has a designated role in the campaign, such as the operator of the hack, the collector of payment, or the leader who oversees the operation.

Of the stolen accounts that the hackers choose to keep, those with at least 50,000 followers are used to keep the scams operational, while those with followers numbering between 10,000 and 20,000 are used as proof to show among peers that a hacker is part of the crew.

Some hackers also sell their hacking know-how in the cybercriminal underground.

How cybercriminals lure potential victims with promises of a verified badge

In another version of the scam, hackers use a fake application form for an Instagram verified badge as a lure. The verified badge is a blue check mark that appears beside the account names of most influencers, celebrities, brands, companies, and other popular entities on Instagram. The badge shows that Instagram has verified the account owner's identity and legitimacy.



Figure 7. The verified badge as shown on Instagram’s official account

To bait a potential victim, the hackers pose as staff members of Instagram (under its parent company, Facebook) and reach out to the target account owner with a message that, unsurprisingly, doesn’t address the account owner by name but instead opens with a generic greeting. The message claims that the account owner can apply for a “blue badge” (verified badge) by filling out an application form, which can be accessed through a URL.

Instagram | Blue Badge Support

Hi, Dear Instagram User. Your Instagram Account has been examined and it has been determined that you are an example for our community. We care about verified accounts for a more secure Instagram. You can contact us by filling out the blue badge application form. When filling out the form, make sure you fill in the correct information or we may not be able to assist you. Application Form:

<https://igcreativeservice.com/5313646785/>

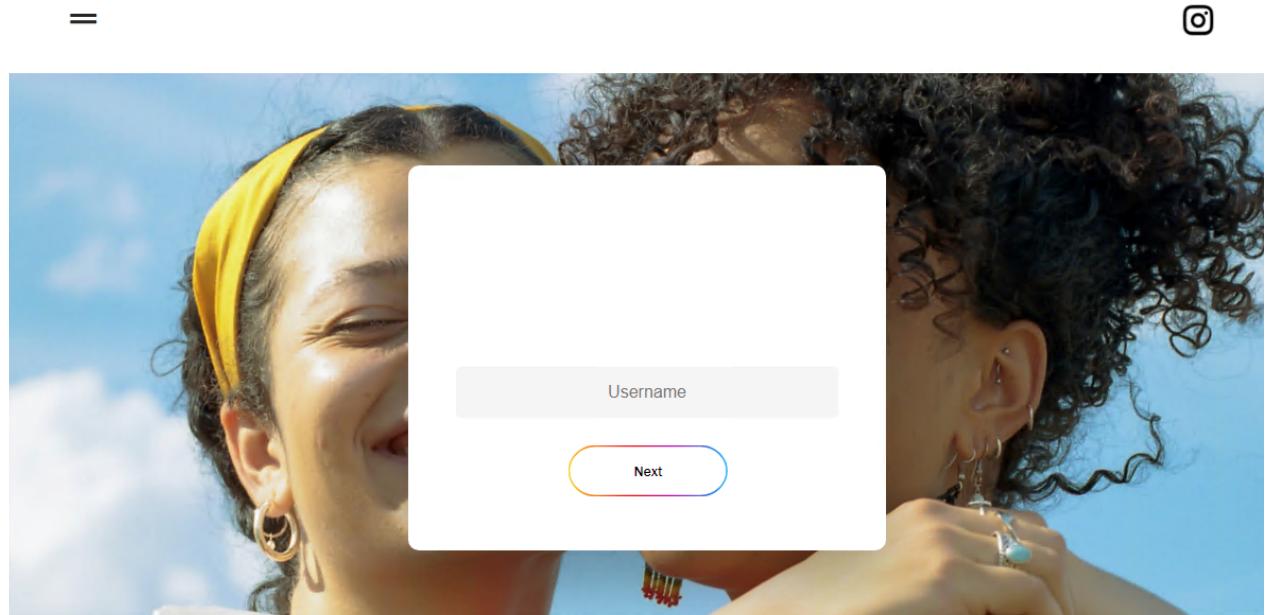
FROM

F A C E B O O K

Support ID : 76458434 Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025 USA

Figure 8. A message from the hackers supposedly offering a target account owner the chance to apply for a verified badge

The URL leads to a page that requests the potential victim’s username. As in the previously discussed scheme, here the page also doesn’t verify whether the username is from an actual Instagram account.



Download for IOS / Android

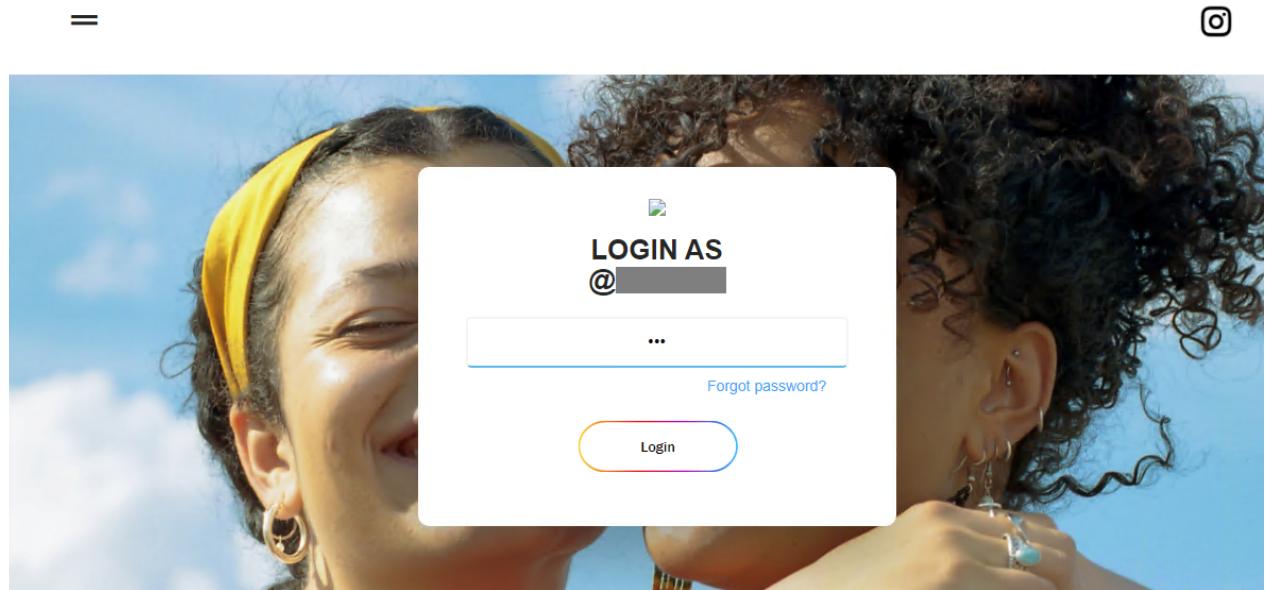


[About Us](#)
[Features](#)
[Community](#)
[Business](#)

[Creators](#)
[Blog](#)
[Help](#)
[Brand Assets](#)

Figure 9. A phishing page that requests the target account owner's username

Selecting “Next” on the page leads to another page that requests the user’s password. This supposedly logs the user into their own account. However, this doesn’t actually happen and the page aims only to harvest the user’s password. The page likewise doesn’t verify whether the password is valid.



DOWNLOAD FOR IOS / ANDROID

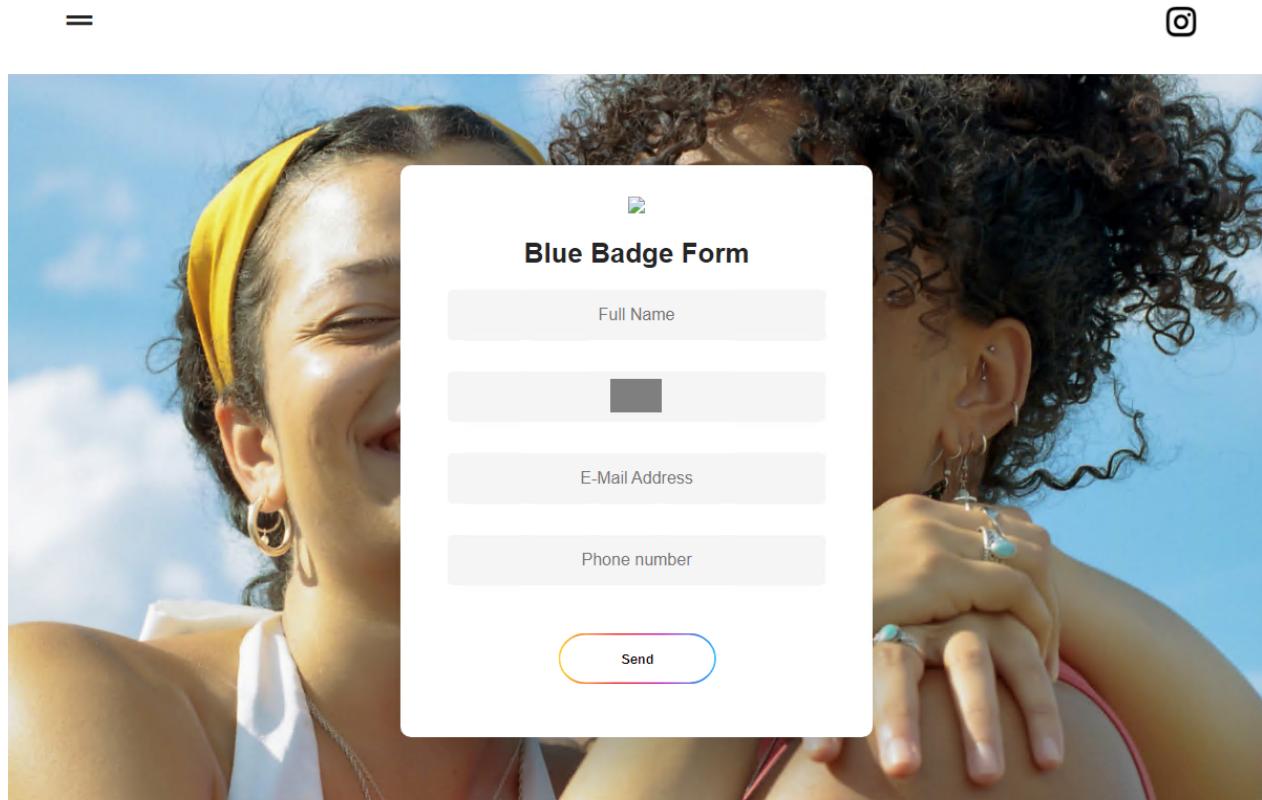


[About Us](#)
[Features](#)
[Community](#)
[Business](#)

[Creators](#)
[Blog](#)
[Help](#)
[Brand Assess](#)

Figure 10. A phishing page that requests the target account owner's password

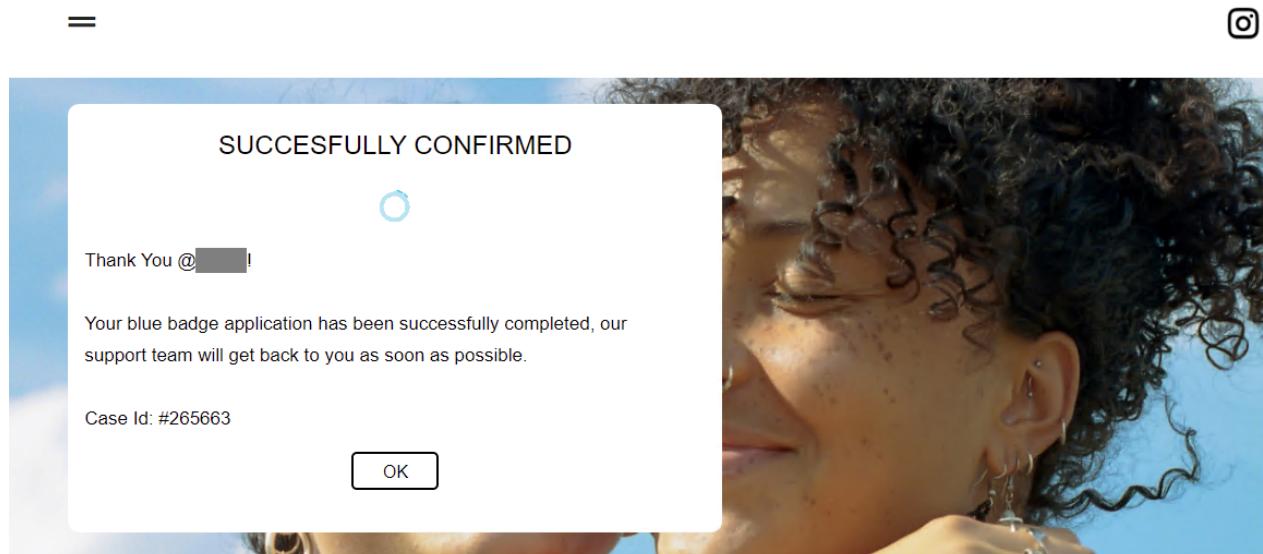
Selecting “Login” leads to a “Blue Badge Form” that requests the user’s full name, email address, and phone number. The form also shows the previously entered username.



Download for

Figure 11. A phishing page that requests the target account owner's full name, email address, and password

Selecting “Send” leads to a page that supposedly confirms for the user that their application for a verified badge has been submitted.



Download for IOS / Android



About Us

Features

Community

Business

Creators

Blog

Help

Brand Assets

Figure 12. A fake confirmation page for the target account owner's supposed application for a verified badge

Selecting “OK” leads to the section on copyright on the actual Instagram support site, as in the previously discussed scheme.

Interestingly, upon investigating the phishing URL through VirusTotal, we found out that the IP address used for the scheme is also linked to a URL that's apparently related to a Covid-19 scam

URLs		
Scanned	Detections	URL
2021-07-02	0 / 88	https://igcreativeservice.com/5313646785/
2021-06-17	0 / 88	https://igcreativeservice.com/5313646785/appeal/
2021-06-22	1 / 88	http://covidhelpservice.com/

Figure 13. URLs related to the IP address linked to this scheme (Source: VirusTotal)

How cybercriminals abuse a hacked Instagram account

Hackers can exploit a stolen account in many ways, including:

- Demanding payment supposedly in exchange for account restoration. As mentioned earlier, the hackers can demand payment, after which they will (supposedly) give the account back to the owner.
- **Scamming the victim's contacts.** The hackers can assume the identity of the victim and reach out to the victim's contacts to send phishing links or directly solicit money.
- **Selling the account in illicit markets.** Interested buyers can purchase the account to propagate their own scams or to push their propaganda.
- **Using the account for their operations.** The hackers can change the name of the account into something that resembles Instagram's tech support and take advantage of its huge following to convey credibility.
- **Asking for lewd photos or videos from the account owner.** The hackers can demand obscene content from the victim. They can then use this content for extortion, selling, or catfishing on online dating sites.
- **Brandishing the account as a trophy.** The hackers can simply use the account as proof of their success that they can show to their crew or to future victims.

How to keep accounts secure

Cybercriminals never run out of tricks for deceiving their targets. Fortunately, many platforms are introducing more security features to safeguard users' accounts. Instagram for one has recently launched its Security Checkup feature, which guides users through a series of steps that can help protect their accounts. These steps include reviewing login activity, profile information, accounts that share login information, and recovery contact information.

Besides efforts from the teams behind apps and websites, users can secure their accounts by following basic security recommendations.

Users are advised to set up two-factor or multifactor authentication. With this enabled, hackers would not be able to gain access to an account even if they have the password. Instagram and many other sites have configurable settings for this.

Users are also advised to never open links in emails and messages from unfamiliar sources, as these links may lead to phishing sites.

Users can check the affected service or website's official support page for more information in case of account hacking or deactivation.

Users can also employ solutions for added layers of security. Trend Micro™ Cloud App Security enhances the security of Microsoft Office 365, Google Workspace, and other cloud services by detecting malicious URLs (such as phishing sites) hidden in the contents and attachments of emails. Trend Micro™ Worry-Free™ Services prevents

credential-phishing messages and other email threats from reaching the network by employing machine learning and other techniques. Trend Micro Security offers protection for home users against email, file, and web threats on their devices.

Indicators of compromise

URL

- helpappealsupport[.]com
- igcreativeservice[.]com/5313646785/