FAQ

https://campus.barracuda.com/doc/93201619/

What is an exception?

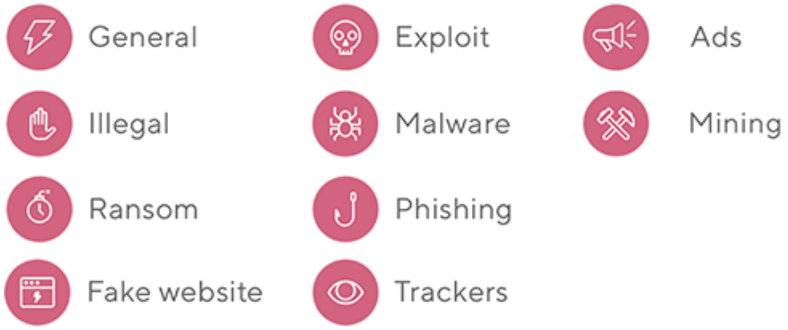
Exceptions are sites that you wish to block or allow access to on a one-time basis. You may change the status of an exception at any time. For example, you can block access to a site that CloudGen Access does not consider a threat based, like adult content or YouTube. Or, you may allow access to a site that CloudGen Access blocks.

> Always be cautious when allowing access to sites that are potential threats.

What does this icon mean?

CloudGen Access brings transparency to all your network traffic, allowing you to see domains visited by the applications on your device. Some of these domains may be collecting your information for marketing purposes. CloudGen Access passes the safe links and blocks the malicious ones, as well as ad and tracker domains, to protect your privacy and security. You can see the allowed and blocked domains in the Activity screen.

Blocked Domains



All mobile applications on your device, and the websites you visit, generate background traffic. This includes hosting services or other sites required to deliver the app or website to your device.

Allowed Domains

Domain

Banking

Why do I need to set up VPN?

Be sure to set up the VPN in your CloudGen Access settings. The VPN is a vital component of CloudGen Access's security checks. We are not a traditional VPN. We do not route any traffic to servers and do not receive or retain any user data. We use the VPN to identify fake Wi-Fi networks and other network irregularities that could compromise your personal information. Your privacy is very important to us. Network inspection, removal of harmful domains/IPs, removal of rogue Wi-Fi networks, and all security checks are performed on your device locally, so all information on the device stays private.

You can check your IP address with the CloudGen Access VPN turned on or off. It will be the same. (https://www.whatismyip.com/)

How does it work?

CloudGen Access will block and send a notification in real-time when a user taps/clicks on a phishing site. This alert will provide information on the site, informing users instantly about the attack in detail.

The common tactic of any deceptive attack is an immediate call to action. Phishers and cyber-criminals all ask a victim to do something, whether it is to “call XX so we can fix it,” “click on this link so we can change your password,” or “click on this link so we can reverse the fraudulent charges.” CloudGen Access intercepts such call-to-action points. The user is advised regardless of whether the site they tapped is fraudulent or not. Our product is evolving to where we now intercept phone numbers and SMS messages to alert users if they are fraudulent.

Why should I allow notifications?

Notifications are very important for CloudGen Access users. We let you know each time we block a threat, like a suspected phishing site, when a Wi-Fi network is compromised, or when a website

seems suspicious.

Be sure to keep Notifications turned on to safeguard your personal security.

What is smishing?

SMS phishing or “smishing” is a criminal activity in which attackers try to obtain personal information such as username, passwords, and tokens via SMS/text message scams.

What is a wetware attack?

Wetware is a term used by hackers to describe a non-firmware, hardware, or software approach to getting the information they want to pilfer. Wetware intrusions happen when a hacker exploits employee trust, predictable behavior, or the failure to follow security protocols. It can be a spear phishing email, a crooked employee, or a file found while Dumpster diving - and, of course, all kinds of things in between. Whatever it is, there is a human being involved.

There are many flaws in human perception, and some of these flaws are applicable to everyone. Cyber-criminals are continuously testing these flaws. One such flaw is "Typoglycemia". This refers to when the words or letters of legitimate companies are changed to steal credentials or information. For example: "gmall" instead of "gmail".

Here is a sample sentence: Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

What assets are at risk?

In the area of consumer security, financial assets represent the riskiest class of assets, especially payment and trading apps (e.g., PayPal, Venmo, Square, Coinbase), with social media accounts a close second.

Attacks fall into two categories:

- An attacker goes after your financial assets to confiscate information and sends it over to the attacker's account.
- An attacker goes after your personal accounts (e.g., photos, videos) and tries to collect a ransom from you.

In the area of enterprise security, there are fewer incidents, but they are much more sophisticated and therefore more consequential. In other words, attackers go after executives of a business to place themselves in a transaction, which are referred to as "CEO whaling attacks" or "business email crime" (BEC). Attackers insert themselves into an email thread or a voice conversation/teleconference and trick the victim to wiring the money to another account. Essentially, the attacker is "man in the middling" and changing some information on the invoice or talking to the finance person and tricking them into wiring the invoice to another account.

What kinds of threats come through mobile devices?

Account takeover attacks (that utilize phishing, smishing, vishing) and rogue Wi-Fi or cellular networks.

What is phishing?

Phishing is a form of fraud that uses both social engineering and subterfuge, and aims to steal personal identity data, financial account credentials, or any other valuable data. Although phishing emails and messages appear to be sent from a reliable source, they usually contain malicious links or attachments. The victims are then prone to click on malicious links or download attachments. The consequences of these events can lead to installing fraudulent software, or having login credentials or account information stolen.

To run a successful phishing attack, an attacker can use link manipulation techniques, or URL hiding. By creating a malicious URL, which at first glance appears to be legitimate, attackers trick victims into clicking on the link.

Another phishing tactic is a link-shortening technique, using services such as Bitly in order to hide the link destination.

To register malicious domains, attackers also use different alphanumeric characters, which when read quickly appear to be look like the legitimate domain name. This technique is called homograph spoofing, where numbers 0 or 1 can be replaced by the letters O and I.

How to spot a phishing email

If the received email or message contains a link, do not click on the link immediately before checking where it might take you. Navigate your mouse over the link (or click and hold on your mobile device) to see whether the link's destination is legitimate. Be especially aware if the email appears to be coming from a financial institution. We advise you to go to the main organization's website, and if you have an account there, log in using your credentials and check whether you have received the same message in your inbox. If the same message is there, then there is no reason to worry.

- Check if the email or a message requests you to share personal information. If yes, do not share any data by replying to the message.
- If you do not know who the sender is, do not click on any signature links identifying the source, but independently check the website and do a bit of research about the company.
- Check if the email or a message contains grammatical errors. This is frequently a sign of a phishing email.

Figures

1. icons.png
2. icons1.png