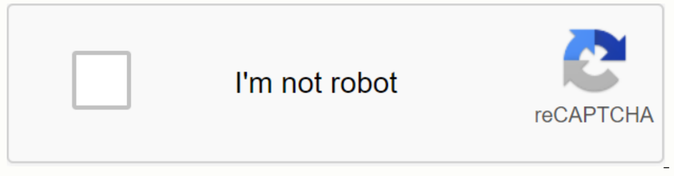

Continue

First security services logo

More Partners Top Graphics: Nick Douglas (My Brand New Logo)Get Ready To... Stand by... Running a small business is hard work, but we're here to help. Welcome to Work Smarter, a one-stop shop for tips and tricks to help small business owners save time and energy. If you need a public-facing logo for your business, one that will appear on signs and prints and ads, one you and your customers will see every day you work, then you should get it professionally designed for hundreds (or thousands) of dollars. If you just need something to put on your Facebook page and your monthly accounts but don't have design skills or Photoshop, then you can get out by customizing the logo on a free or cheap page. We tried more and found three that work well enough to recommend. My brand new logo When we had to create a fast and dirty business logo in the next two hours, we would choose My brand new logo. The site charges 50 euros (about $57) for quality copies of the logo. Honestly, this seems fair because MBNL is both slick and very flexible. Just a touch of personalityTell MBNL your business name and slogan, and give it some tags so you can choose a snippet of art. Then choose a layout — some are much better than others — and customize. The website will randomly present you with 20 options, or you can upload more. Everything is customizable, including rows, icons, sizes, positions, patterns, and colors. You can match any icon and color scheme with any layout. And you can put the logo off. You can't load your own assets. The impressive variety within very specific categoriesKost logos on this page has the same feel. If you fit the benign design style that has recently gentrified the world - the WeWork/Starbucks/Airbnb style that balances elegance, modernity and approachability - you'll fit in. And this is exactly the brand that I wanted for my soup subscription service, SoupPass.Please increase to appreciate my custom waves of fragrance textureSho download package 50 euros includes high resolution and vector files with different colors and sizes options, as well as some social media resources. These are all things you would reasonably expect from a paid job. HatchfulHatchful is a free online logo maker (also on iOS/Android) from the small business management suite Shopify. If you can't imagine paying even $50 for your logo, you can still find something decent here. Tell Hatchful your business name and slogan and where it will appear (online, on business cards, blown up on signs) and select some logo styles. The adjustment options for Hatchful are limited. You can only select specific color and font combinations. This may help you not to play house and all day to adjust. But I didn't find enough hard text options to withstand the senseless spirit of the heartless. heartless. save the logo and make an account, Hatchful sends you a folder of download funds, including picture 1200x1200 and versions with different dimensions depending on how you say you use the image. If you've chosen social networks, this includes funding for Facebook, Twitter, Pinterest and LinkedIn. You'll get some horrible cropped options, as well as more ly-potable, where your logo sits in the middle of the banner:The package also includes a tiny favicon for your site, which in my case ridiculously included the company's name and slogan:You can return later and edit or re-download your property. You'll probably want to do some tweaks when you see your logo on different sizes and configurations. FreeLogoServicesFreeLogoServices is not free! It costs $40 to download a high-quality copy of your log. In general, we would recommend the other two cities first, but if they are not your style, then FLS seems a fair option. Its greatest strength is its selection process, which makes more sense than the order of operations in other places. First, the website requires the basic type and layout of the logo you want. When you narrow the selection, the background options change to customization. Styles on FLS are much more traditional, more late 90s MS Publisher. Sometimes that's what you want. Clip icons also come with their own more colors, a little more flash than standalone colors and gradients of other cities. There are fewer literal options. I went with a logo that subtily evoced two aspects of my funeral stylists business, Tomb and Haircut. The FLS download package includes high true copies of your logo in colors and black & white, and with or without transparent background. The site also offers business cards that start at $20 for $100. Again, reasonable and service. You get what you pay for. If all these designs seem cheesy, then we should probably spring for the right designer. Try looking at Dribbble, Behance or 99designs. And get ready to pay much more than $57 – good designers cost good money, and you should. Several Top Security partners failure, password violations, false attacks and phone scams -- if you follow the news, may seem like the inevitable pitfalls of life today. There are, however, many tools that can give you tools to protect you and your family from digital crime. We've put together some of the most trusted services that won't empty your wallet in the process. When using a public Wi-Fi network, virtual private network (VPN) services can protect your computer's IP address when you surf the Internet, encrypt browsing information, and prevent most (though not all) espionage. With broad platform support and high-speed Internet speeds, IVPN is well worth an annual fee of $100, and discounts are common. Keep all accounts safe and healthy with services that Create strong, individual passwords that you save for you, all secured for one master password. LastPass is affordable ($24 a year for premium plan), easy to use and supported on almost all major platforms. The company has grown in recent years with some previously paid features, such as syncing on all your devices, free. When it comes to privacy, not all instant messaging platforms are created equal. If secure communication is necessary, follow signal. With end-to-end encryption, the ad-free app locks everything about your conversations, from the words you use to people who can't stop them. You can also send messages using the Self-Destruct Timer, which is deleted after the space you select. The free extension of uBlock Origin prevents text tracking bites, commonly known as cookies, from sticking to your browsing history so that advertisers can't create a profile of your preferences while browsing. UBlock makes it easy to enable ads from the site you want to support, or sites that require ads to run, such as Hulu. Most regular, free email accounts are fine for average users, but if you need to be extremely confident the messages you send and receive are 100% protected, check the secure email services below. These services provide an easy way to keep emails private, with secure, encrypted email provided. ProtonMail is a free, open source, encrypted email provider based in Switzerland. It works from any computer through the website and also through Android and iOS mobile apps. The most important feature when talking about any encrypted email service is whether other people can catch up with your messages or not, and the answer is firmly no when it comes to ProtonMail, because it has end-to-end encryption. No one can decrypt encrypted ProtonMail messages without your unique password, including protonmail employees, their ISP, INTERNET service provider or government. ProtonMail is so secure that you can not recover emails if you forget your password. Decryption happens when you log on, so the service doesn't have the resources to decrypt emails without your password or recovery account in the file. ProtonMail also does not store IP address information. With an email service without a log, such as ProtonMail, you can't trace emails back to you. Additional useful features include: Sucking messages with pictures and formatting rich text. Keyboard shortcuts. Download the PGP keys. The free version of ProtonMail supports 500 MB of email storage and limits usage to 150 messages per day. Pay for Plus or Visionary for more email space Priority support, labels, custom filtering options, auto reply, built-in VPN protection, and the ability to send multiple emails every day. The expert plan is also for organisations. If you are seriously concerned about email privacy, CounterMail offers a secure implementation of OpenPGP encrypted email in your browser. Only encrypted emails are stored on counterMail servers. In addition, servers (based in Sweden) do not store e-mail on hard disks. All data is stored only on CD-ROMs. This method helps prevent data from leaking, and the moment someone tries to interfere directly with the server, the data may be lost. With CounterMail you can also set up a USB flash drive for further email encryption. The decryption key is stored on your device, and this is what's required to sign in to your account. So decryption is impossible even if a hacker steals your password. Additional useful features include: changing account settings. Create forms to send results to e-mail. Supports e-mail filters. Uses anonymous e-mail headers. Works in the browser and through the iOS app. Includes multiple identities to receive mail in the primary mailbox. The added physical security of the USB device makes CounterMail less easy and convenient to use than other secure email services, but you will get IMAP and SMTP access that you can use with any OpenPGP-enabled email program, such as K-9 Mail for Android. Buy a plan to use the service after one week's free trial. The test includes 100 MB of space. Hushmail is another encrypted email service that has existed since 1999. E-mail messages are secure and locked behind the most common encryption methods. Not even Hushmail can read your messages; this can only be done by someone with a password. With this service, you can send encrypted messages to Hushmail users as well as nonuse who have accounts with Gmail, Outlook Mail, or other similar email clients. The web version of Hushmail is easy to use and offers a modern interface for sending and receiving encrypted messages from any computer. When creating a new Hushmail account, select from different domains that you want to use in the title, such as @hushmail.com, @hushmail.me, @hush.com, @hush.ai, and @mac.hush.com. Additional features include: Works online or iOS; mobile web version works on all mobile platforms. Sign up to receive notifications of received emails in any other email account, including a non-Hushmail account. Supports e-mail signatures. You can make unlimited email aliases with the @nym.hush.com domain name to hide your identity online. There are both personal and business options when you sign up for Hushmail, but neither is free. However, there is a free trial that is valid for two weeks, so you can try out all the features before you buy. Mailfence is a security-centered email service that has end-to-end encryption to ensure that you and your intended recipient cannot read your messages. The service includes an e-mail address and a web interface that includes OpenPGP public key encryption. Create a key pair for and manage key storage for the people you want to secure email. This openPGP standardization means that you can access Mailfence using IMAP and SMTP with secured SSL/TLS connections through an e-mail program of your choice. You can't use Mailfence to send encrypted messages to people who don't use OpenPGP and aren't available a public key. Additional features include: Doesn't use ads. Your email settings are open for customization and compression. Purchase credit memos for sending faxes and text messages. Import messages in EML format. Send mail through the address you used to sign in (for example, gmail address). For online storage, the free mailfence account provides 500 MB, and paid accounts offer enough space, as well as the ability to use your own domain name for your Mailfence email address. Mailfence's software is not available for inspection because it is not an open code, making it less secure and private. Mailfence stores your private encryption key on Mailfence servers, but insists that it cannot be read because it is encrypted with your pass phrase (via AES-256) and there is no root key to allow the service to decrypt key-encrypted messages. Mailfence uses servers in Belgium, so the company can only be forced through a Belgian court to disclose private information. Tutanota is similar to ProtonMail in its design and security level. All Tutanota emails are encrypted from sender to receiver and decrypted on device. A private encryption key is not accessible to anyone else. This email account is all it takes to share secure emails with other Tutanota users. For encrypted email outside the system, specify a password for the recipient to use when viewing the message in the browser. This interface also allows them to respond securely. The web interface is easy to use and understand, make the email private or not with one click. However, there is no search function, so it is impossible to search for past e-mail messages. Tutanota uses AES and RSA for email encryption. The servers are located in Germany, which means that German regulations apply. Free accounts can create an email account with a Tutanota domain, and paid plans can create custom domains. The Tutanota domains are: @tutanota.com, @tutanota.de, @tutamail.com, and @tuta.io. Additional features include: custom folders for organizing messages. Supports attachments. Passwords are salted and dissolved with bcrypt. Several features in this service are only available in paid plans. For example, premium edition allows you to purchase up to 5 aliases, while Team's plan extends your storage to 10 GB. If you're using an email service that provides end-to-end encryption, you've taken a big step toward a secure and private email. Additional steps you can take to difficult for dedicated hackers include the following precautions: Beware of keylogging software that covers what you enter on These programs can prevent encryption if the password is all a hacker needs to access the account. Don't leave unguarded mobile devices or computers. Also, make sure that devices are protected by strong passwords or biometrics and don't allow guest accounts or similar unprotected access. If supported, you can also add two-factor authentication. Pay attention to social engineering. Phishing attempts often come by email, instant messaging, VoIP, or social media messages and can be designed or customized specifically for you. These communications are tricks to give you personal information, such as passwords and bank information. Do not write or share passwords. Never write a password that lets you decrypt secure e-mail messages unless you save it in a secure password manager. Manager.