

Internet Safety for Survivors of Domestic Violence and victims of stalking



If you are reading this, chances are you have been the victim of violence or stalking where the threat of re-offence is significant. Or you know, or work with, such victims.

For you, the internet can help provide greater safety and a wealth of resources, but it can also hold additional risks.

In order to stay safer you will need to change your online activity. The following guidelines cannot guarantee to keep you from harm, but they will help you learn how to take additional precautions, to better protect your anonymity, location, and identity.

In this document...

- About abusers
- Clean up your computer
- Socializing in email, IM, social networks, chat forums etc.
- Risk with posting photos
- Using mobile phones safely
- E-shopping
- Getting help

Let me start by saying that you do not have to have a degree in computer science to dramatically improve your safety. Consistently applying a few simple rules, and staying vigilant, will do a lot to help you stay safer online.

About Abusers

There are four primary forms of abuse - emotional abuse, financial abuse, reputational abuse, and physical abuse of people or property. If you are the victim of relationship violence, the abuse may include all of these forms.

It is likely that you know your abuser, they may be a family member, have a charming as well as a violent side, and they may be very adept at bullying people, gaining sympathy, or telling a good story to get what they want - which if you are in hiding, will be information on how to find you.



Your abuser may not be particularly savvy about technology, but they don't have to be, to successfully employ many methods of finding you. Setting up a new profile that includes the city where you live, exposing your friends list, blogging about what you're doing, leaving an 'away' message on your email saying where you're going: these are all things an abuser might be able to see. And it may not be you who exposes your whereabouts, someone else may accidentally do it for you. Not only do you need to learn to hide information, but anyone who knows where you are, needs to learn to keep your secret too.

Clean up your computers, mobile phones, and vehicles



If your abuser is someone you know - a spouse, ex, colleague, friend, etc. - they may have placed tracking or monitoring or spying software on your computer, laptop, handheld device, or mobile phone.

The tracking method may be in the form of a specialized spying product that has been secretly installed, or it could be that they have turned on "parental controls" making you the 'child' account so that everything you do is reported to them. No one has to be a technology genius to use either of these options.

Even if you don't think your devices have been compromised, your safest bet is to assume they have been, and that everything you do or say online, including your passwords, calendar, email, contacts, is being monitored until you've cleaned up these devices. If you aren't technically savvy, you may want to have a TRUSTED friend or family member help you, or use a pc dealer or repairer to do this for you.

Next, if you do not have up-to-date security software installed, do so now. If cost is an issue, use one of the excellent free alternatives (see get help section). Set the security software to automatically update, then your machines have the best protection possible. Do NOT leave your computer unprotected; this is like leaving your front door unlocked.

Make sure your wireless connection is password protected with a new, strong passwords. (See the section on safe passwords to learn how).

Once your device(s) are clean and secure, Create new, strong passwords for your administrator accounts and be sure you are the only person with access. Set a new password to log on to your computers and phones so that no one but you can use them.

Do not skip these preliminary precautions. If your machine is forwarding all your information to your abuser, the safety steps outlined in the rest of this guide cannot help you.

Once you've accomplished these steps you can be reasonably confident that your online actions aren't monitored, and your safety has significantly increased.



Socializing online

Having a support network is critical to anyone who has experienced physical or emotional trauma, and the internet provides great opportunities to find this kind of support, and have it available 24 hours a day. It's hard to call family, friends, counselors or supporters in the middle of the night when grief, panic, or anger strikes, but someone is probably online. There are also forums and access to information. You just need to do so safely.

This section contains information about how you can stay safer when using various internet services that enable socializing.

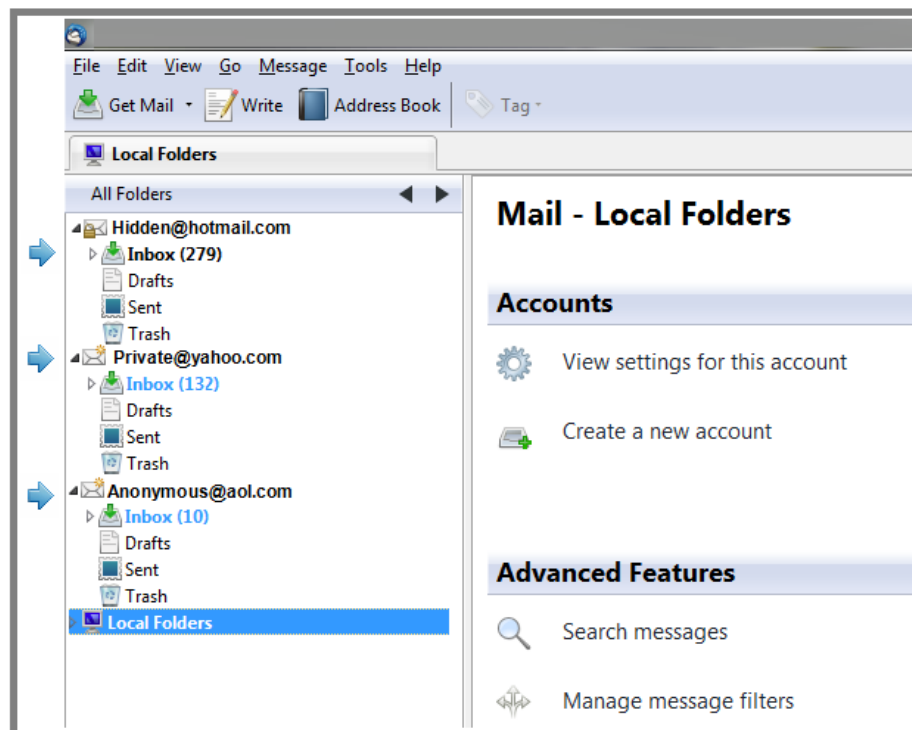
Email -create a new account

If your abuser knows your personal email address, simply blocking their email account from contacting yours is a good first step, but it is not likely to be enough. They can constantly create new accounts to use to contact you.

Consider creating one or more new email accounts:

1. Create one email account for your most trusted contacts.
2. Another account for when you register on websites
3. An email for financial accounts e.g. online banking or PayPal.
4. Lastly, create one account for contacts that you and the abuser both know – they may give your new email to the abuser.

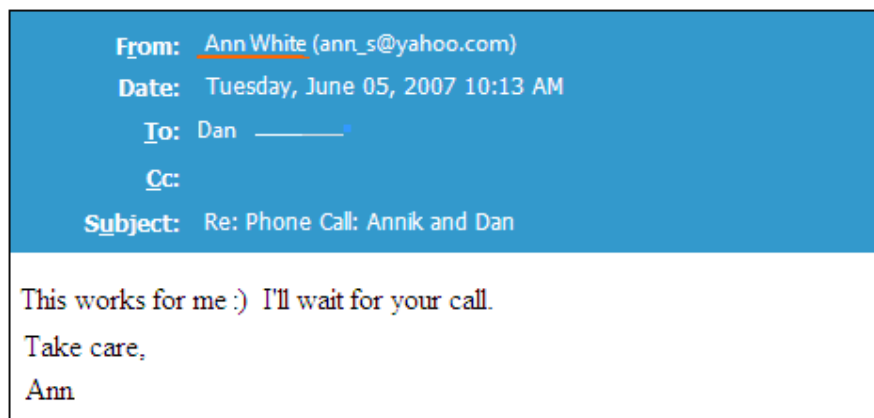
Having multiple accounts is safer because if your abuser gets hold of one, the others remain safe. Managing multiple email accounts does not need to be difficult. In most email services' settings you will find an option to import email from other accounts - even if they are from other service providers. For example, you may have a Hotmail account, a Yahoo! account, and an AOL account. By importing all your accounts into one service, you can easily manage them all from one spot. See the Illustration below as an example of how you can see multiple accounts through your primary email account.



Stay anonymous when creating new email accounts

Unless an email account is related to your professional life where you need to use your name, make your email names anonymous, so they do not identify you - not by name, birth date, age, location, ethnicity, work descriptor (like teacher, dancer..) or other characteristic. And you shouldn't create an email name that is sexually suggestive, or expresses emotion.

Once you've created the new email accounts, check to be sure the service doesn't expose your real name as well. To find out if your email service displays your real name, send yourself an email and check to see if your real name is displayed alongside your email name in the sender field. Real names are displayed by default on e-mails you send from many of the major e-mail services. In the example below, you'll see how a woman who chose "ann_s" as her email name, also had her full name - Ann White - exposed.



The good news is that you can usually change the setting to hide your real name. Below are the instructions for doing this in Windows Live (hotmail).

1. In Windows Live, click the *Options* button on the right side of the screen (next to the Help icon with a question mark on it).
2. Click the *View and Edit Your Personal Information* link.
3. Click the *Settings* link on the left side of the screen.
4. Click the *Profiles* link under Account Information.
5. Click *Edit Your Account Profile* link
6. On the Account Profile page, either delete your first and/or last name or replace them with other information that doesn't identify you personally. You can use any alphanumeric characters (A-Z; 0-9) and any of the special characters on your keyboard except for :, <, >, ,, (,), ", \$, and !.



NOTE: Other e-mail services have their own procedures for changing the display of your name in sent messages. If your email service displays your name and you can't find how to hide this, e-mail your provider or search online for the proper procedure. If the provider doesn't allow you to hide your real name, use a different service.

Keep your email private

There are two aspects to keeping your email private: how strong your passwords are, and **who you share your email address** with. Think carefully who you give it to and which sites you use it on. You want to be able to contact, and be contacted by, those who support you, but avoid the abuser getting your email address.

Strong passwords are critical

If you lived with the abuser, or they had access to your computer at some point in time, you should assume that any passwords you have were compromised. Change them all. **Now.**

Safe passwords don't have to be hard to create; they just have to be hard to guess.

Creating a strong password, changing a password, or using multiple passwords makes many people anxious because they believe it requires memorizing multiple complex passwords, such as Wts4e_79PBa3. This isn't the case. Here's what you need to know to make strong and memorable passwords.

Safe Password safety rules:

Use different passwords for each site so that, if one password is hacked then they won't be able to use the same password on other accounts.

Passwords that are short, simple words or include numbers that relate to personal information (such as birth date, address, pets names) are easy to guess. Don't use 123456 or abcdef either.

Don't use weak passwords – you don't want them to break into your account!



How to create easy to remember secure passwords

Use a long Phrase

Coming up with a long phrase can make it easy to remember. "It was a dark and stormy night!" Now just use the first letter Iwadasn, You can change the "a" into "&"

Use words to create a pattern

Use words to create a standard pattern it is an easy way to create passwords for every website you use. Create a new password such as "<master pass>" "<username backwards>" "<first 3 letters of a website>"

eg master pass = K£te

user name (joebloggs) = sggolbeoj

website = evictims.org

the new password = K£tesggolbeojevi.

Remove the Vowels

Take a word or phrase and remove the vowels from it.

eg, "eat the cheeseburger" becomes "tthchsbrgr"

Use the Keyboard

If your password doesn't use the Q, A, or Z, you can hit the key to the left of your password. Or to the right if you don't use the P, L, or M.

Eg. **evictims** using keys to the left becomes **wcuxruna**.

You can also try using above and to the left; so **evictims** becomes **3f8d58jw**

Develop a code

Take the name of the website and then add the last four digits of a friend's home phone number to the end. (Don't use your own phone number, since a clever hacker could try the same)

You need **different passwords** for different websites. You can use software that keeps a list of your passwords e.g. www.keepass.info. But it's okay to keep a list of your passwords, just be sure to first change the existing passwords and put the new list in a safe place that's not near your computer or pinned up on the wall!

Security questions

Many sites ask you to answer a 'password hint' or 'security' question from a drop-down list. Unfortunately, many of the questions ask for answers that can be found in publicly-available information such as your place of birth, a school you attended, or your mother's maiden name. In cases of domestic or partner violence, chances are that your abuser will not only know these answers, but also know the correct answers to questions like the name of a favorite pet, your best friend in primary school, etc.

Answering any of these questions correctly could allow your abuser to get into, and take over, your account.

If none of the security questions allow you to give an answer that others couldn't discover, *use a fake answer - just remember it!* The service doesn't know if your answer is correct, it verifies only that you can repeat the answer you gave before. For example, what is your mother's maiden name? Purple Butterfly. Your first car? Purple Butterfly. The city you were born in? Purple Butterfly.

how much information is still exposed. We see her name, her photo, her comment, her age and location, when she last logged in (indicates she is still active on the account) and her URL further exposes her name. As any of this information is updated the abuser has the opportunity to learn more.

This profile was set as private so only friends can read the profile. There is some information you can't make private on social networks.

IM – Instant messaging

Create a new account

If you use Instant Messaging (IM), use your new email account(s) to create a new IM account. When setting up the account, be sure to choose a nickname/user name that does not identify you. Do not use identifiable information in your URL. Do not use your own photo or any photo that could be uniquely associated with you, and don't indicate your location. Set your account settings to be private (friends only) and be careful when adding friends so that your abuser does not have access through a friend's login. If you choose the privacy option that allows friends of friends to see your account, your abuser will likely be able to see it.

Social Networking sites and Forums

Social sites that allow you to share and get support are important tools for victims of abuse, but you have to be extra cautious when using social networks. If you or your friends are careless, it can lead the abuser to your new door/workplace or other location.

We don't recommend anyone using Facebook. Their privacy settings are such that you aren't safe using Facebook.

Delete existing accounts!

If you don't delete the account you may be tempted to check these accounts periodically, but if your abuser is aware of these accounts, they will continue to monitor them to glean information *even if they are set to private*. If you want to continue using an existing social networking site or forum, create a new account to avoid being tracked by an abuser.

The illustration below helps you see how information is exposed on 'private' sites. 'Jessica' set her MySpace account to be private. Yet, look at



Social networks

It is very difficult to stay safe on a social network. You need to restrict the number of friends you add to account. Check to make sure **each of your friends have set their privacy settings to “only friends”**. Warn them that your abuser may use fake names or names of friends to get them to add him. If they already have your abuser as a friend DO NOT add them.

Forums

Don't go back to forum or chat rooms that you used before. The abuser will look for new members and can tell by the way you phrase things it is you. There are a lot of forums online so it should be easy to find a new one. Look for forums where you can keep your profile private.

Twitter and blogging



Twitter and micro-blogging sites are designed to be public – in other words you can't make them private. Even if you are careful, what you say about your location, activities, or emotions, added together they may provide too much information to a determined abuser. That is why we suggest not using them.

Social networks like Facebook and Twitter have implemented location functionality that, if turned on, might show where you are whenever you post. Be sure that any location functionality in any online service you use is OFF. (This includes shutting off Bluetooth functions on mobile devices.)

Get a feel for what it will take for you to successfully and safely use the site. Look at the site's privacy settings and policies, do they leak too much information by making things public in your online profile, do they make it easy for you to notify them of any problems? Do a search by putting in “social network” privacy problem. If the site doesn't provide strong privacy settings, pick a different site.

Creating new accounts is easy

With a few simple guidelines you'll be able to create an anonymous account.

- Omit any information that can identify you. In general, only fill in required fields, and, if these fields can be seen or used in a search, use fictional information about location, gender etc.
- Don't put up a profile picture and abuser may see your picture through a friends list.
- Carefully select your privacy settings to be sure you are not visible or searchable to anyone you have not expressly said you want contact with.
- Only invite **very trusted** people to join you. You should have a limited amount of friends.



Share cautiously

Sharing information online is all about considering two factors: what you are sharing (how sensitive the information is) and who you want to share the information with. If you give out general information or restricted to only selected friends (who have their privacy restricted also), there is less risk in sharing it. However, if you say things that give your location, work or where you going out etc that information could leak out to your abuser.



Here are some categories of information you may want to consider as you determine what you're comfortable sharing or having others share about you publicly. This list isn't all things you need to consider but should be designed to get you to think about what information you give out and to whom.

Information you should keep private

- Your name and the names of family members and friends:
- Ages and genders: Of you, your children, or other family members
- Identifying information: birth year, birth date, zodiac sign, city, schools, work or clubs
- Emotions: Abusers are probably very interested in whether you are happy or sad, or lonely, angry or feeling independent, have a new friend or are falling in love
- Addresses: This includes home and work addresses, as well as any other location you visit regularly. Consider what information should be exposed if you are announcing - or attending - an event for a birth, wedding, graduation, or death. Any event that the abuser could learn of and assume you will attend poses a real concern. Whether or not they 'attend' they may be watching and follow you home.
- Phone numbers: This includes home, mobile phone, work number, and friends' numbers
- Personal numbers: Bank accounts, credit cards, debit cards, PINs, passport, birth date, wedding date, insurance policy numbers, car registration plate, NI number and more.
- Information rich photos: A perfectly innocent photo can reveal more than you think. You might put yourself, family members, or friends at risk by posting photos that show where you go out or work, for example.

Remember, even when you are careful to ensure that no individual blog or forum post contains information that gives you away, the accumulated information over time may do so. Periodically review the entire 'set' of information for risks, and delete anything that when combined is too much.

Others may be sharing information about you

Remember that you aren't the only one sharing information. Search the Internet for information about you.

What others say can give away important information


Family and friends may post information about you in blogs, on genealogy sites, and on photo-sharing sites, for example. You may not want people to know you were fired or your mobile number or how you were out partying. But this is **the type of information friends post about you**. A stalker will also make comments to get your friends to reveal information about you.



HisWiseGirl Yes, @Annabeth_C, Percy was **drunk**. And Thalia (me) kept zapping him until **he** jumped into the lake. xD
8 minutes ago from Twitterrific



Whatleydude @sean376 I thought you got fired?
about 3 hours ago from TweetDeck

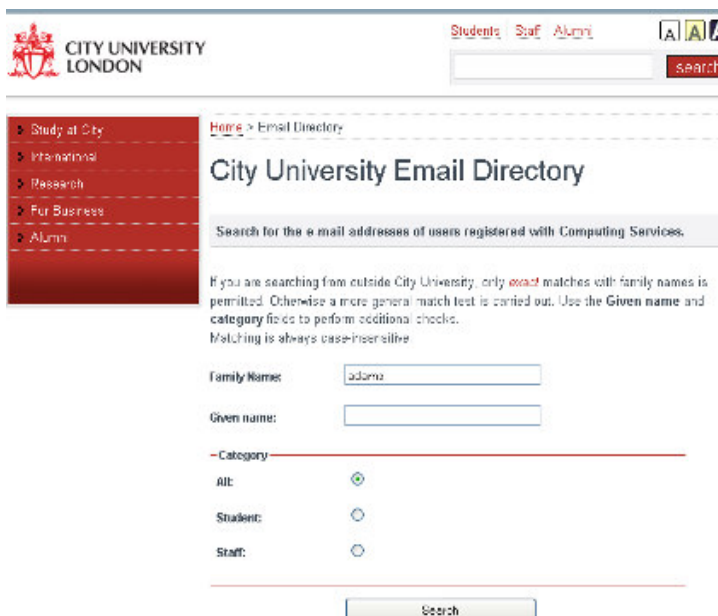


Riverview2066 I believe this **is** Max M [REDACTED] **mobile** phone **number** if anyone **is** interested - 041250160

Employees

Employers may share information about you on the company's website. If you are working in a big company, you may also want to be cautious about how much is visible to other employees on an intranet. When you attend a conference, be sure your name is not exposed on an attendee list on the conference website or documents. If you are a speaker, you may need to take extreme caution when arriving and while at the conference to never be alone, and when leaving to be sure you are not followed.

Students



The screenshot shows the City University London website's email directory search interface. At the top, there is a navigation bar with 'Students', 'Staff', and 'Alumni' links. Below this is a search bar with a 'search' button. The main content area is titled 'City University Email Directory' and includes a search prompt: 'Search for the e-mail addresses of users registered with Computing Services.' Below the prompt, there is a note: 'If you are searching from outside City University, only **exact** matches with family names is permitted. Otherwise a more general match test is carried out. Use the Given name and category fields to perform additional checks. Matching is always case-insensitive.' There are three input fields: 'Family Name' (containing 'adams'), 'Given name' (empty), and 'Category'. The 'Category' section has three radio buttons: 'All' (selected), 'Student', and 'Staff'. A 'Search' button is located at the bottom of the form.

Be sure any school you attend does not expose your information on their web sites. This may be in the form of a student directory at universities or colleges or it may be through photos and captions, listings of sports team members, event dates, etc. This information may be about you or one of your children - either way, you become locatable.

The illustration screenshot here shows how universities often expose information about students. City University has a publicly available email directory. Anyone can simply type in the name of a student and get that person's email address, what course they are studying.

Identifying information exposure in images

Photos and videos often share far more information that people realize. What an abuser sees may be considerably more than you do. They will look in the background for clues – have you moved, who is that with you, when you go out -where do you go etc. You and your friends need to make sure photos online don't compromise your safety or cause your abuser to escalate his actions.

Using mobile phones safely

It is hard to imagine how we managed before mobile phones. They also can help an abuse trace or harass you. Stay safer by doing the following:



The safest mobile phone is one that cannot be traced back to you – Pay as You Go phone. Abusers are often very good at creating convincing stories for companies about why they need your contact and location information and 'helpful' staff may provide it. If the company does not have your information, they cannot expose it.

Get a pay as you go phone because these do not require a contract so you don't have to show ID, give your name or address.

Protect your phone number. Abusers will try to contact and locate you through other people if they cannot contact or locate you directly. Insist that the people you entrust your phone number with do not share it. You may want to consider using more than one SIM card so you can use different phone numbers for the types of people you contact.

Consider some of these features before you get a new phone.

Mobile phone features

Look for these features

- Does the phone or device have Internet access? If so, it is critical that nothing you post online from your phone identifies you or your location.
- Is the phone or device Bluetooth enabled? Blue-tooth is a technology that allows a mobile phone to seek, discover and 'talk' to other Bluetooth-enabled devices in the area. This means that you may receive unwanted content or your location might be accessed without permission. Set your phone to 'not discoverable' using your Bluetooth setup menu, or if not using Bluetooth, just turn it off.
- Does the phone or device have location (GPS) capability? GPS can be a lifesaving tool if it allows a *trusted* contact to see if you have been abducted. That said, *extreme caution* should be used if you are considering a location service that allows friends or strangers to track your location, learn your patterns, and expose you, or your property, to privacy invasions or physical harm.
- Does the phone have a camera? You need to review every single image for identifiers before sharing them: does the image include a building, landmark, or scene that might indicate where to locate you?
- Does the phone allow you to block numbers?

If the cost of purchasing a new phone is an issue, many domestic violence and safe shelters can provide you with a donated phone.

E-shopping



You should close all current e-shopping accounts and open a new one using your new email and secure passwords. You don't want the abuser to gain access to your new delivery details, credit card etc.

Abuser uses eBay to track down victim

"A victim's partner knew her eBay account name. He waited until she ordered something. He called the seller saying the item did not arrive. He asked the seller to confirm the address, and then went

round and beat up his ex-partner leaving her blind in one eye".

Finding trusted resources and getting help

E-Victims.Org helps victims of e-crime and other online incidents www.e-victims.org. They also have a list of free anti-virus software.

Women's Aid Federation of England Offers support, advice and information on all aspects of domestic violence.
Website: www.womensaid.org.uk
Telephone: 0808 200 0247

National Refuge
Website: www.refuge.org.uk
Telephone: 0808 2000 247

National Centre for Domestic Abuse - free, legal aid, including injunctions
Website: www.lcdv.co.uk
Telephone: 0844 8044 999
Mobile: Text NCDV to 60777

Respect - Men's Advice Line for men experience domestic violence
Website: www.respect.uk.net
Telephone: 0808 801 0327

Shelter - Housing charity, includes links for those trying to leave abusive relationships
Website: <http://england.shelter.org.uk>
Telephone: 0808 800 4444

Rights of Women
Educates women about their legal rights.
Website: www.rightsofwomen.org.uk
Legal helpline: 020 7251 6577
Sexual violence helpline: 020 7251 8887

Victim Support
Website: www.victimsupport.org.uk
Telephone: 0845 30 30 900
Scottish domestic violence helpline
Website: www.scottishwomensaid.org.uk
www.scottishwomensaid.org.uk
Telephone: 0800 027 1234

Wales domestic abuse helpline
Website:
www.walesdomesticabusehelpline.org;
Telephone 0808 801 800

Northern Ireland domestic violence helpline
Website: www.niwaf.org
Telephone: 0800 917 1414

Irish Women's Aid
Website: www.womensaid.ie
Telephone: 1 800 341 900

Samaritans
24-hour confidential emotional support for anyone in a crisis.
Helpline: 08457 909 090
Ireland helpline: 1850 609 090
Website: www.samaritans.org.uk

E-Victims.org provides training courses on Internet Safety for Survivors of Domestic Violence and Stalking Contact Jennifer@e-victims.org

This guide was done in conjunction with Jennifer Perry, Managing Director of E-Victims.Org and Linda Criddle a leading US Internet Safety advocate and President of LookBothWays inc www.ilookbothways.com.