All About STIs: Socially Transmitted Infections

Keep Your Valentine's Day Free of Social Media Malware

This Valentine's Day, Fortinet is taking a look into the world of the socially transmitted infection, a new kind of electronic STI, which can cause almost as much pain as that other kind. Keep reading to find out how social media can be used to spread infections and learn tips to help keep you safe today.

Introduction

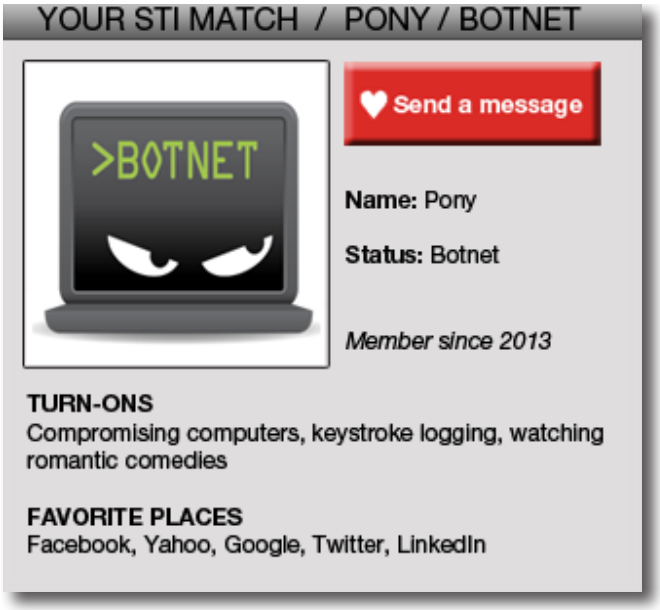
If you only use social media for keeping track of the activity of friends, family, and celebrities, then your experience is probably pretty safe, at least as far as your computer is concerned

But you would also be in the minority of social media users. Social media has evolved from sharing details about your life to something that is far more dangerous: sharing links. Linking, and the subsequent clicking of these links, has changed the Internet landscape, and malware can now be spread ten times more effectively through social media than it can be through email. Because of this, it is important to know what these STIs can do and how you can prevent them.

The Bait

Social media is built on trust. A friend list is made up of people you would trust with your personal information; where you are, what you're doing, who you're with.

Trusting your contacts leads to you trusting the links that they post, and you may even click on them without thinking about it. This gives STIs the opportunity to infect you while you're trying to check out the latest Internet sensation (most likely, a cute cat video).



The Tricks

There are a number of tricks that malware uses to get itself noticed and onto your computer, including:

- Sending messages out about popular topics, such as celebrities or recent news stories, in order to get more views.
- Adding malicious extensions to your browser that can hijack your social media accounts.
- Making downloads appear to be from legitimate sources, such as fake updates for Flash.
- Disabling your computer's antivirus and sending you to compromised websites.
- Packaging malicious software with legitimate software and advertising it on social media as a special deal.

The Results

Once you've caught an STI, the most commonly attacked items are your user credentials. Password theft makes the news frequently, such as the recent attack by the Pony Botnet which resulted in the theft of two million credentials for sites such as Facebook, LinkedIn, and Twitter.

Having a password stolen can be risky, especially for anyone who uses the same password in multiple places, such as online shopping sites or even work computers (of course, you shouldn't be reusing passwords at all, but more on that later).

Attacks also frequently involve the installation of malware that can later be used to add your computer to the botnet that caused the attack, causing it to grow even more powerful. Botnets are also often used to generate online buzz for companies or individuals through social media posting, an activity known as 'like farming.'

Treatment Plan

If you just came home to find your Twitter account sending out spam in a foreign language, or you see any other signs of having caught an STI, do the following immediately:

1. Change the password of the affected account to one that is secure, more important, and unique. Do the same for any other accounts that use the same password.
2. Visit the applications page of the social media site the account was on and revoke access privileges of any apps you don't recognize.
3. Run virus and malware scans on your computer.
4. Let your friends know that your account was compromised and that they should be careful about any strange messages they receive from you.

How to Practice Safe Surfing

Now that you know more about STIs, here are the best ways to prevent infection in the first place:

1.) Always Use (Unique) Protection

Having secure passwords goes beyond the regular precautions of mixing letters, numbers, and special characters.

The most important thing is to have every password be unique to the account it is associated with. This way, having one account breached won't cause all your other accounts to be vulnerable. It is also important to not use passwords that can be easily guessed, such as the generic "123456" or "password," or birthdates (which can often be found online).

A good way to secure your password is to use a password manager. Password managers not only securely store your passwords but can also create new ones that are difficult to guess.

Also be sure that you have secure secret questions that you will remember but that cannot be easily guessed by casual acquaintances. For extra security, memorize incorrect answers to common security questions.

Once you have set a secure password, you should change it often and never share it. If for some reason you have to share your password, do not send this information across a network, and change it as soon as possible.

2.) Make VD Stand for Virus Detection

All computers need to have anti-virus and anti-malware programs installed and kept updated. It is also recommended to scan your computer on a regular basis, especially if you often download files from the Internet.

3.) Think Before You Click

If you see a friend post something that seems unusual for them (like your spelling-obsessed aunt's posts being filled with typos), **don't click it!** Instead, check with them to see if it's legitimate. Be especially careful about links from high profile accounts, such as celebrities, since they make great STI targets. You should also avoid clicking links in generic posts, like "hey, check this out!"

You should also keep an eye on URLs, to make sure they match where you're supposed to be. Watch out for malicious websites that will put a familiar name within their URL to fool you into thinking it's affiliated with that site. If a link uses a short URL, hover over it with you mouse to see the address in full before clicking it.

Finally, if you ever see an ad for a deal that seems too good to be true, it probably is.

4.) Pass Information, Not Infection

Protect yourself by protecting your friends, who are the ones most likely to put you at risk of catching an STI. Make sure they know what social malware is and what they can do to prevent them (perhaps by passing this paper along to them).

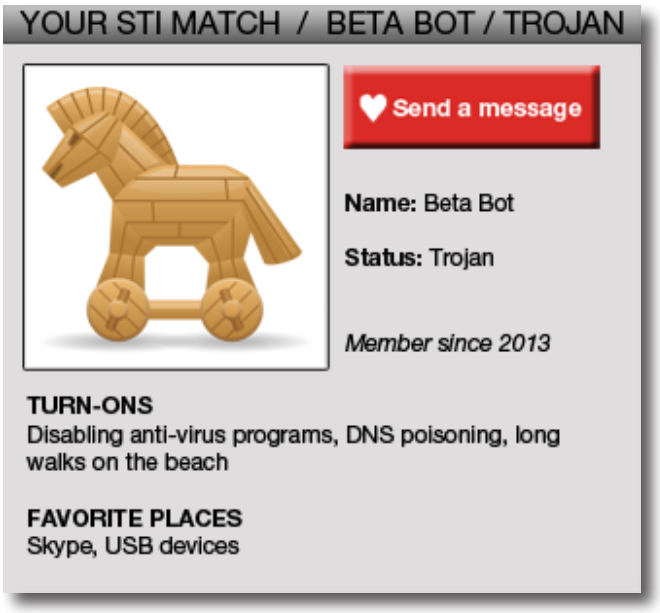
If you ever have reason to believe that one of your contacts has had their account compromised, let them know immediately and make sure they know what to do to regain control of their account.

Also, if you ever see something suspicious on a social media site, find the contact page and let the administrators know so that they can take care of it and spare others from being infected.

5.) Other Tips

Here are some other tips for protecting yourself from STIs:

- Log out of your social media accounts when you are done using them, especially on public computers.
- Make sure you know who all your social media contacts actually are.
- Keep your computer operating system and applications updated, especially your browsers and any other programs that can access the Internet.
- Only download applications and updates from their original source.
- Use a pop-up blocker on your Internet browser.
- Use a browser plug-in that limits the sources allowed to run JavaScript code.
- Research any new apps that you want to download to see if they are safe.
- Stay alert about new social media malware attacks and learn how to prevent them.
- Don't ignore a vulnerability just because it isn't listed as critical.
- If children use your computer, use parental control software and, if possible, supervise them to make sure they aren't clicking something they shouldn't. You should also educate them about the risks.



Conclusion

Socially transmitted infections are getting more sophisticated every day. As a result, it is almost impossible to be 100% protected, unless you consider complete Internet abstinence a solution.

However, if you practice safe surfing and use your common sense, you can greatly reduce your chances of getting infected by social media malware (and get back to watching those cat videos in peace).

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia
Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480