The Event and Our Response

On May 3rd, 2019, during one of our clinics in Ensenada, we suffered the theft of a laptop. The theft occurred via a break-in of a vehicle which was parked at Broncos Steakhouse in the early evening hours.

Regrettably, the theft of the laptop may lead to the discovery of a file which lists the user name, the e-mail address, and the encrypted password of each volunteer registered on our volunteer web site.

Within an hour of the theft, we disabled our volunteer website, and on may 5th completely shut down the virtual machine where the website was being hosted. Access to the website remains down until further notice, so that we can further assess the situation and develop a response. We will be moving the website to a new host and invalidating any access keys to ensure that it cannot be logged into by unauthorized persons.

What Was Compromised

One or more files on the laptop contained a list of volunteer usernames, encrypted passwords, and e-mail addresses.

Your full name name, address, and phone number(s) are not included in the password file. We never store (or ask for) social security numbers, by policy. We do not have a record of, nor do we see, the credit card numbers that you enter when registering for a clinic. These transactions are handled by a separate, third party web site, and will continue to be processed in this way.

What Action Should You Take?

Out of an abundance of caution, we suggest that you change passwords on websites that share or are similar to the password that you chose to use with your thousand smiles volunteer account.

See "**Technical Considerations and Risk**", below, for further information that may be helpful in deciding what response you should take.

What We Are Doing To Respond

1. We currently have the website down until we can put systems in place to reliably force a reset of everyone's passwords. The web site, and the host that it runs on, will remain down indefinitely.

2. We reported the theft to the local police in Ensenada and described the laptop in the hopes that they will find it and notify us. If that occurs, we will take all necessary steps to get the laptop back in our possession.
3. We are in the process of bringing up a copy of the laptop from backups taken right before the incident, and will evaluate this system to determine if there are risks beyond those described in this message, and respond if that is the case.
4. We will take steps to ensure that an incident like this does not happen again. This will include adopting better procedures related to the handling, storage and transport of data that you provide us when signing up, and registering for our clinics.
5. We will continue to never ask you for, or store passwords, social security numbers, or other information that is irrelevant to our mission, and which might put you at risk, if compromised.

We take your privacy and the security of our site seriously. We apologize for this incident, and for any convenience this may have caused you. We will work to ensure a stolen laptop will not put us in a similar situation in the future.

Technical Considerations and Risk

If you are not sure if you need to change passwords, the following is an attempt to clarify your risk in the context of our site, the password you chose, and the circumstance of the theft itself.

First of all, if your Thousand Smiles password is the same as your e-mail password (e.g., the password you use with your email account such as hotmail.com, gmail.com, etc.), then we strongly recommend that you reset your e-mail password on those e-mail systems/sites. This is because a successful attack on the password file would reveal your password on that e-mail site, and allow access, both passwords being the same.

All of the passwords on the system are encrypted. Technical factors that influence the ability of the thief to obtain the plain-text passwords from these encrypted passwords include:

1. The encryption algorithm. We use what is considered strong encryption algorithms, but their strength is affected by the remaining factors in this list.
2. The length of your password (longer is better)
3. Use of special symbols in your passwords, and mix of upper/lowercase. More is better.
4. Use of dictionary words. Passwords which contain words that are humanly recognizable or are a combination of humanly recognizable words (e.g., 123dog, mypasswordabc123) are easier for attackers to exploit.

Simply put, if the password you used was weak, the encryption method is less effective at sustaining a well-funded, determined attack.

There are non-technical risk factors surrounding this incident to also consider:

1. We believe (but can't be sure) that the goal of the theft was likely focused on the value of the laptop, not necessarily on the value of data that might be found on the laptop.
2. The thief is most likely unaware of the fact that data of this sort is present on the laptop and it would take some level of technical skill to find it.

3. If found, a certain level of technical sophistication would be required to properly understand how to approach the task of decrypting these passwords.
4. Moderately secure passwords in the database would require significant time and computing power to decrypt.
5. Selling of the e-mail addresses to spammers is a possible outcome, but it is hard to say if the small number of e-mail addresses involved would be of any value to anyone, and recoup the costs required to crack them.

But we can't be sure that the laptop did not fall into the hands of someone who is capable and determined in finding a list of e-mail addresses and passwords, and has the technical and computing resources to exploit them them. Or that the laptop or its contents might be sold to someone with these skills and resources. Given the uncertainty of the situation, we suggest password resets on your important websites and accounts, again, out of an abundance of caution.

if you have further questions, please contact us by e-mail at thousandsmilesvolunteer@gmail.com, and we will try our best to answer them.

Thousand Smiles Board of Directors