17439

South Hadley Dental Associates, Inc.
15 Dayton Street
South Hadley, MA 01075

5/7/2020

[redacted]
[redacted] MA [redacted]

Dear Mary,

We are writing to inform you that an unauthorized person may have accessed records containing your personal information in April 2020. This potentially accessed information includes your social security number.

We regret that this has occurred, and we have worked with our IT provider, our email host, and our employees to improve our network security. Because your social security number may have been exposed in this incident, we would like to offer you up to eighteen months of complimentary credit monitoring. If you wish to accept that offer, you can either (a) enroll in the program of your choosing and provide proof of enrollment, at which point we can reimburse you, or (b) wait for further instructions from us, as we are currently in contact with a credit monitoring company to arrange services for you.

If you receive an email or other communication that purports to be from South Hadley Dental Associates but includes an unusual request for financial or personal information (for example, access to an Amazon account), it would be prudent to contact us by phone before you respond or click a link. We are also enclosing a publication from the Federal Trade Commission about recognizing and avoiding phishing scams which you may find useful.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. There is detailed information appended to this letter about the process of placing a security freeze on your credit report, for which there is no charge.

We are committed to addressing any questions or concerns that you may have about this situation. You may write to us at 15 Dayton Street, South Hadley, MA 01075, email us at shdental15@gmail.com or call us at (413) 536-4455. We will promptly respond to any communications.

We apologize for this unfortunate incident, and we are working hard to maintain your trust in us.

Sincerely,

Marjorie Block DMD

South Hadley Dental Associates, Inc.
Marjorie Block, D.M.D.

Information on Security Freezes

Both Massachusetts law and federal law allow consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Credit reporting agencies are not permitted to charge you to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. The address[es] where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Social Security card, pay stub, or W2
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

How to Recognize and Avoid Phishing Scams

Scammers use email or text messages to trick you into giving them your personal information. But there are several things you can do to protect yourself.

How to Recognize Phishing

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful. The FBI's Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one year (https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120).

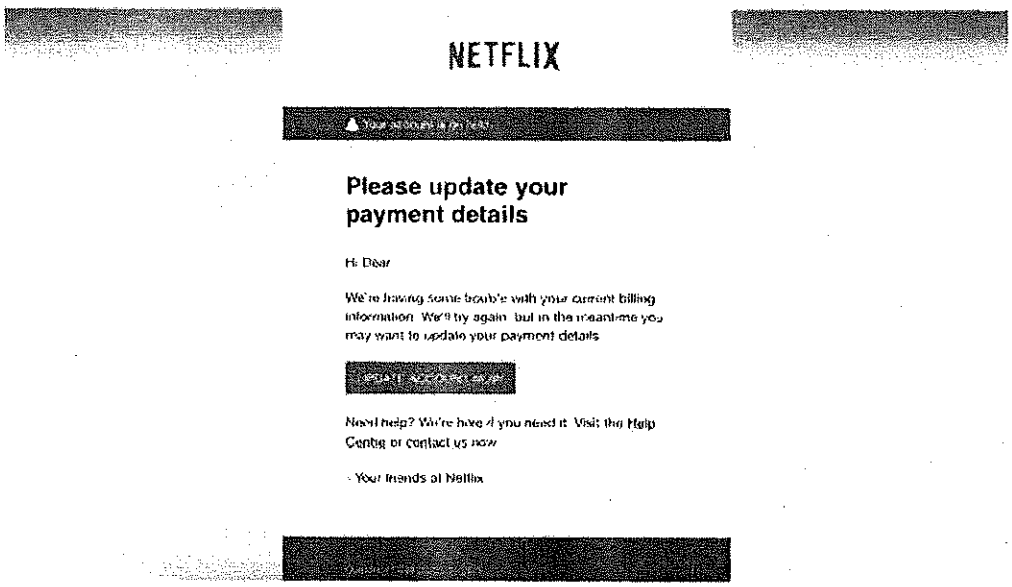
Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice (https://www.consumer.ftc.gov/blog/2017/05/fake-emails-could-cost-you-thousands)
- want you to click on a link to make a payment
- say you're eligible to register for a government (https://www.consumer.ftc.gov/blog/2018/03/western-union-refunds-scam-alert) refund
- offer a coupon for free stuff (https://www.consumer.ftc.gov/blog/2014/11/free-pizza-nope-just-free-malware)

Here's a real world example of a phishing email.


NETFLIX

Please update your payment details

Hi Dear

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details

Need help? We're here if you need it. Visit the Help Centre or contact us now.

- Your friends at Netflix

Imagine you saw this in your inbox. **Do you see any signs that it's a scam?** Let's take a look.

- The email looks like it's from a company you may know and trust: Netflix. It even uses a Netflix logo and header.

- The email says your account is on hold because of a billing problem.
- The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email invites you to click on a link to update your payment details.

While, at a glance, this email might look real, it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can harm the reputation of the companies they're spoofing.

How to Protect Yourself From Phishing Attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it's a good idea to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

Four Steps to Protect Yourself From Phishing

1. Protect your computer by using security software. Set the software to update automatically (https://www.consumer.ftc.gov/blog/2019/06/update-your-software-now) so it can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication (https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication). The additional credentials you need to log in to your account fall into two categories:

- Something you have — like a passcode you get via text message or an authentication app.

- Something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up your data (https://www.consumer.ftc.gov/media/video-0105-back-it-dont-lose-your-digital-life) and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

What to Do If You Suspect a Phishing Attack

If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: **Do I have an account with the company or know the person that contacted me?**

If the answer is "No," it could be a phishing scam. Go back and review the tips in How to recognize phishing (#recognize) and look for signs of a phishing scam. If you see them, report the message (#report) and then delete it.

If the answer is "Yes," contact the company using a phone number or website you know is real. Not the information in the email. Attachments and links can install harmful malware.

What to Do If You Responded to a Phishing Email

If you think a scammer has your information, like your Social Security, credit card, or bank account number, go to IdentityTheft.gov (https://www.identitytheft.gov/Info-Lost-or-Stolen). There you'll see the specific steps to take based on the information that you lost.

If you think you clicked on a link or opened an attachment that downloaded harmful software, update your computer's security software (https://www.consumer.ftc.gov/articles/0009-computer-security#update). Then run a scan.

How to Report Phishing

If you got a phishing email or text message, report it. The information you give can help fight the scammers.

Step 1. If you got a phishing email, forward it to the Anti-Phishing Working Group at reportphishing@apwg.org (mailto:reportphishing@apwg.org). If you got a phishing text message, forward it to SPAM (7726).

Step 2. Report the phishing attack to the FTC at ftc.gov/complaint (https://www.ftccomplaintassistant.gov/).

May 2019

Related Items

- Why Report Fraud? (https://www.consumer.ftc.gov/media/video-0143-why-report-fraud)
- How to File a Complaint (https://www.consumer.ftc.gov/media/video-0054-how-file-complaint)
- How to Spot, Avoid and Report Tech Support Scams (https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams)
- Faking it — scammers' tricks to steal your heart and money (https://www.consumer.ftc.gov/blog/2015/07/faking-it-scammers-tricks-steal-your-heart-and-money) (Blog Post)
- How to Recognize and Report Spam Text Messages (https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages)