Dental Managers Society Newsletter
We Welcome Medical Managers!
September 2024

Hackers Probably Have Your Social Security Number from a Massive Breach

Last year, we reported that we were part of the Harvard Pilgrim Health breach. At that time, we provided instructions on how to maneuver these challenges.

With the announcement of another possible breach affecting billions of individuals, we are reissuing and updating this information to help you stay safe.

This new National Public Data breach is monumental, and it's safe to assume you're at risk. The hackers put the entire database — which includes Social Security numbers, full names and addresses on the Dark Web for sale and when it didn't sell for the $3.5m that they wanted, so they handed it out for free!

Below is a verified website where you can check if your data was included in the breach. The compromised data appears to be from an older backup, as it may not contain your current address information.

https://npd.pentester.com/

Here's why it matters:

If your Social Security number is stolen and used for someone's gain, like opening up a loan or getting a job, start with the Federal Trade Commission's IdentityTheft.gov ***(https://www.identitytheft.gov/Steps***). Fill out the form there, and you'll get an entire plan for how to recover your identity and protect yourself going forward.

The IRS also has a place to report if you suspect someone is using your SSN: ***Identity Theft Central*** (**https://www.irs.gov/identity-theft-central)**. Major red flags to watch for? You receive a tax form for a job you didn't do or you submit your taxes and there's already something on file. You know things are bad when both the FTC and the IRS have dedicated portals to help you because someone is using your SSN and stealing from you.

ACT SMART I.T.
Helping You Benefit From Today's Technologies

Our recommendations:

- **Change your password(s), especially if you have used your passwords on other sites.**
- **FREEZE your accounts at the three major credit bureaus.** This will keep anyone (even your self) from opening a new line of credit. Don't worry; you can unfreeze your credit or temporarily lift a freeze for a set amount of time like when you are ready to apply for a credit card, and allow access to lenders.

Equifax—https://www.equifax.com/personal/credit-report-services/credit-freeze/

TransUnion—https://www.transunion.com/credit-freeze

Equifax—https://www.equifax.com/personal/credit-report-services/credit-freeze/

- **Activate credit alerts**
- **If your identity has been compromised or misused,** file an Identity Theft Report with your

Continued on page 3

Letter from the Editor

Pam Snell,
DMS Advocate

Hello and Happy September!

As we start winding down and gearing up for the last quarter of the year, I have to admit, the gorgeous weather makes it hard to fully let go of summer. It seems like the sunshine just doesn't want to quit, and honestly, I'm not complaining!

While hurricane season is typically on our minds this time of year, things have been quiet so far—fingers crossed it stays that way! Even though there's no immediate storm on the horizon, it's always good to be prepared. That's why I've put together a handy infographic, *"Safeguard Critical Documents and Valuables"*, which you can download from our website here: https://actsmartit.com/safeguard-documents-valuables/ It's a resource from FEMA and is useful any time of year. While you're on the site, don't forget to browse the **Infographics Archive** for other valuable resources I've created over time!

David and I are also spotlighting a must-read article this month: *"Hackers May Have Stolen Your Social Security Number in a Massive Breach."* It's the kind of information that'll keep you up at night. Be sure to use the verified link on the front page to see if you were affected. Unfortunately, David and I were. Thankfully, we froze our credit years ago, so while we're not panicking, we're still staying vigilant—and you should too.

We're also happy to feature **Vinny Pircio** from Wareham Banker again with another edition of *Scam Alert!*. This month, he's focusing on the *Fake Bank Call Scam*. Even if you're unlikely to fall for it yourself, it's a good idea to share the article on page 7 with any friends or family who might be more vulnerable. Scammers are always finding new ways to trick people, and it never hurts to be one step ahead!

On a lighter note, I've been busy updating and refreshing our **OfficeManagersSociety.com** website, which now has tons of new articles that didn't make it into this issue. If you're interested, definitely take a look at what's new!

On the home front, our garden is overflowing despite the lack of rain. We're practically swimming in cucumbers, and I've watched David climb a ladder just to pick the scarlet runner beans! It's been a busy but rewarding harvest.

And we had a little celebration recently—Sarah turned 8 on September 1st! It feels like just yesterday we were sharing her baby photos with all of you. To wrap up the summer, we managed one last trip to Wicked Waves on the Cape, and the kids had an amazing time splashing around at the water park.

What a way to end the season!

local police department.

- **Cybercriminals often sit on their spoils for months** until the turmoil dies down and our vigilance diminishes. Then, they'll use their ill-gotten gains with fewer chances of immediate disclosure. It's not unusual for companies to say that they are unaware of breached information being used at the time they disclose the breach.
- **Your healthcare insurance itself is also very valuable** and can be sold on the Dark Web so stay vigilant.

Minor children may also be at risk. We suggest putting a credit freeze on their accounts at all three national credit bureaus. Since they have no credit on file, a form must be completed and mailed. Although it's more of a hassle than completing your requests online, it is protection that you don't want to exclude. For more information, read:**https://www.equifax.com/personal/education/identity-theft/child-identity-theft/**

THE CURRENT
TECH ALERTS
POWERED BY KIM KOMANDO

Kim Komando issued a special Tech Alert on August 15.

A fake tax form is one thing; most signs of identity theft are more subtle—at least, in the beginning. Here's what to look for, along with steps to lock down your identity and protect your money:

- **Double-check all healthcare communications.** If you get an explanation of benefits (EOB) or bill for services you didn't receive, contact your healthcare provider and insurance company ASAP. It likely means someone is using your benefits for their own care.
- **Treat email requests with caution.** Be skeptical of anything that seems super urgent. It's OK to slow down for safety.
- **Freeze your credit.** *See our ACTSmart tips on page 1*
- **Be wary of "old friends" who appear out of nowhere.** It could be a hacker who happens to have a little (stolen) info. Take the time to confirm they are who they say they are.
- **Make a list of exposed data.** Keep this digitally or on a Post-it. Be suspicious of anyone who references it in an email or phone call. Say the company you financed your car through was hacked. Alarm bells should sound if you get a call out of the blue about a major issue with your loan.
- **Update your PIN and banking login credentials,** even if they weren't involved directly in a breach. Keep an eye on your bank and credit card statements for anything out of the ordinary. Set up banking alerts on your phone, too.

Want to get Kim's Free daily newsletter?
https://join.komando.com/ef9e99759

Would you like a print copy of this article mailed to you?

Go to: https://actsmartit.com/stolen-ss-number/

Avoiding Voting Scams and Safeguarding Elections

Elections are a cornerstone of American society. However, there are bad actors who don't respect the sanctity of our voting process.

In this digital age, election time and voting scams have presented new challenges for the security of our democratic institutions. Here's how you can stay safe online as you prepare to head into the voting booth.

Phishing is on the rise

Traditionally, phishing attempts increase when big events, like elections, are on the horizon. Cybercriminals engaged in phishing often impersonate legitimate entities, like campaigns, to acquire sensitive information. Scammers will send emails, text messages, or social media messages masquerading as official election authorities, political campaigns, or even candidates. These messages may contain false information, request personal details, or provide links to malicious websites.

To avoid falling victim, always be skeptical of unsolicited messages, verify the legitimacy of the sender, and never click on suspicious links. Look to your federal, state, or city governments for official election information.

Spoofed election websites

Malicious actors create fake election websites that closely mimic legitimate platforms to deceive voters. These sites can be used to defraud people by asking for phony donations. They're also created to spread misinformation, collect data, or distribute malware. Access election-related information through official government websites with secure connections (https://) and be extremely cautious about clicking links shared through social media or emails.

Watch for voter suppression tactics

Election scammers have exploited voter suppression tactics to impact how people participate in the democratic process. This includes spreading malinformation about polling locations, voting dates, or eligibility requirements. Always use official government sources when it comes to looking up voting information. Report any suspicious activities to election authorities.

Fake voter registration drives

Bad actors have used social media to fool potential voters into thinking they can vote through a website, text message, or phone. Not only is this voter suppression, cybercriminals might use these tactics to steal your personal data. Scammers may pose online as volunteers or representatives of political parties, manipulating individuals into providing sensitive details. Use federal government resources to register to vote or check your voter information. **No states permit registering to vote over the phone.**

Robocall and phone scams

During election seasons, robocalls and scammers can spread misinformation, intimidate voters, or provide false instructions. They might even ask for money and lead you to believe you are donating to a campaign. Hackers can "spoof" phone numbers and impersonate official organizations – always be vigilant, and you can always opt to donate through verified websites. Be suspicious about unsolicited calls and never share personal information with someone who calls you. **Report** suspicious calls to relevant authorities and consider using call-blocking systems to filter out potential scams.

Help protect democracy

Democracy is precious and protecting our electoral process in our connected age should be important to everyone, no matter the political party. You can help play a part by learning to avoid election scams, reporting any suspicious election-related activity you come across, and teaching others about scams and voter suppression. As responsible citizens, let's embrace our role in ensuring a secure and transparent democratic process for generations to come.

https://staysafeonline.org/resources/avoiding-voting-scams-and-safeguarding-elections/

Grammar for Grownups

Why am I so interested in helping American grownups use our American system of grammar correctly?

As my mother constantly asked, "Didn't everyone learn it in school?"

Well, first of all, no. We didn't, and there are several reasons for that. Yes, the teachers tried, but there's a huge difference between being taught and actually learning.

Second, the last time most of us were exposed to grammar was about eighth grade, after which we were often told by our creative writing teachers that we should just express ourselves and not worry too much about those pesky punctuation details.

And in eighth grade, most of us were 13 or 14, our hormones were raging, and we were likely more interested in the cute boy or girl sitting next to us than listening to any lessons given by anyone over 25. How could we have known then that we'd grow up to care about the stuff teachers taught us, especially stuff like grammar? We couldn't have, and it's been maybe 20, 30, or 40 years since "back then" anyway.

Who remembers exactly what we were taught?

Your nose just twitched …

Third, we often decide how to write or speak based on what someone else does.

The problem with doing that? Most of us are smart, but we're not always smart in the same way. Following the HR VP's way of using semicolons, for instance, might not work, because she's smart as a whip with people and HR issues, but not so smart about American punctuation rules.

Am I right?

And fourth, American grammar is different from other variations of English grammar. We have some punctuation rules (especially those concerning the use of quotation marks) and some spelling (*humor* or *humour, realize* or *realise,* and usage differences that are just part of our way of speaking or writing.

As we are more and more a global community, we often see articles written in a different version, and if we're not sure about our own system, we can get confused about what we're supposed to do here.

So the burning question: Why do I show writers the edits I've made in their content? I want them to learn.

I want writers to look and sound as smart as they are.

Get Susan's booklet
"Colons and Commas and Dashes, Oh My!"
American Grammar and Usage Tips.

Go to ACTSmartIT.com/susan and we'll mail you a FREE copy!

Scam Alert!

With so much of our lives being digital and with more and more of our banking being done electronically, it is more important than EVER to make sure you don't become a victim of fraud.

This month, we're talking about a scam that has been very common in the last few months and has affected many people and banking institutions. It's called the ***Fake Bank Call Scam.***

This scam is one of the more infamous scams that I have seen in the last few months and in my opinion, the most successful for the scammers. This scam starts with a phone call from your banking institution; surprisingly, they can spoof your bank's phone number. For example, you may get a call that will show on your caller ID as the bank's phone number. Any average person would assume that their bank is calling them for a valid purpose, which is how they start earning your trust.

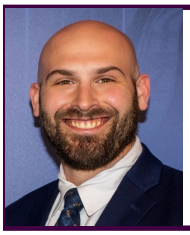
Once they have you on the phone, they will indicate that they are calling from "your financial institution" and ask if you authorized a transaction in a location you have not been to. For some reason, they tend to tell customers that the fraud occurred in New York City. If you hear this, it should raise an immediate red flag. Now, most people would be frustrated, anxious, or even scared. This is part of their plan to get them to trust you.

Next, they will ask you to confirm your debit card number, PIN, and Balance. **Banks will never ever ask for your PIN (or online banking password).** If anyone from a "financial institution" ever asks for a PIN. this is another red flag. Once they have your card number and PIN, they can make a fake card and start charging purchases to your account. As soon as they have this info, it will be too late.

There are ways you can protect yourself from this scam.

- Be aware that this is happening; many people trust their bank, and if they don't know this scam is happening, they are more likely to trust the individual on the phone.
- Listen closely for red flags; some examples are below:
  - Asking for your PIN
  - Asking for an online banking password
  - Saying you've "had fraud in New York City"
- Call a trusted bank representative
  - Reach out to your local banker
  - If you do not have a local banker you are familiar with, hang up MMEDIATELY and call your financial institution to confirm the call.

Fraudsters are everywhere and are getting sneakier by the day. It's more important than ever to make sure you are protected and your hard-earned money remains yours!



Vincent A Pircio, Branch Manager II,

Rockland Trust

2995 Cranberry Highway, East Wareham, MA 02538

Phone (508) 295-6900 | Fax (508) 295-7178

Vincent.Pircio@RocklandTrust.com

UPDATING YOUR POLICIES – The "CROWN ACT"

The acronym CROWN, within the CROWN Act, refers to "Creating a Respectful and Open World for Natural Hair." Such legislation prohibits discrimination based upon hairstyle that is commonly associated with a race or national origin.

While there isn't a federal prohibition at this time, currently around 2 dozen states have enacted this law, including Connecticut, Maine, Massachusetts, New York and New Jersey.

New Hampshire recently enacted the CROWN Act, which takes effect in that state on September 1, 2024.

Two areas where your employee handbook must be updated:

- Employers should be taking a second look at their dress and grooming policies to ensure that such policies do not violate the protections of the CROWN Act.
- This legislation should be referenced within your anti-discrimination policy.

What if certain hairstyles cause a safety problem for your particular business in terms of your legitimate business needs? As always, open communication, with a discussion as to ways to address and adapt to those concerns, must take place.

Attorney Helene Horn Figman combines specialized legal knowledge in employment law with the skills and perspectives uniquely suited to Human Resources Consulting. www.figmanlaw.com

Information about her anti-harassment and anti-discrimination education programs can be found at www.workplaceawarenesstraining.com

This article has been prepared by the Law Offices of Helene Horn Figman, P.C. for general informational purposes only. It does not constitute legal advice and is presented without any representation of warranty whatsoever.

Helene Horn Figman

Law Offices of Helene Horn Figman, P.C.

Employment Law & HR Resource Management

45 Bristol Drive Suite 207, South Easton, MA 02375

FigmanLaw.com hfigman@figmanlaw.com

508-238-2700

In This Issue:

This newsletter was thoughtfully edited by Susan Rooks, the Grammar Goddess, so we can look and sound as smart as we are.

Susan Rooks
The Grammar Goddess
https://www.linkedin.com/in/susanrooks-the-grammar-goddess/