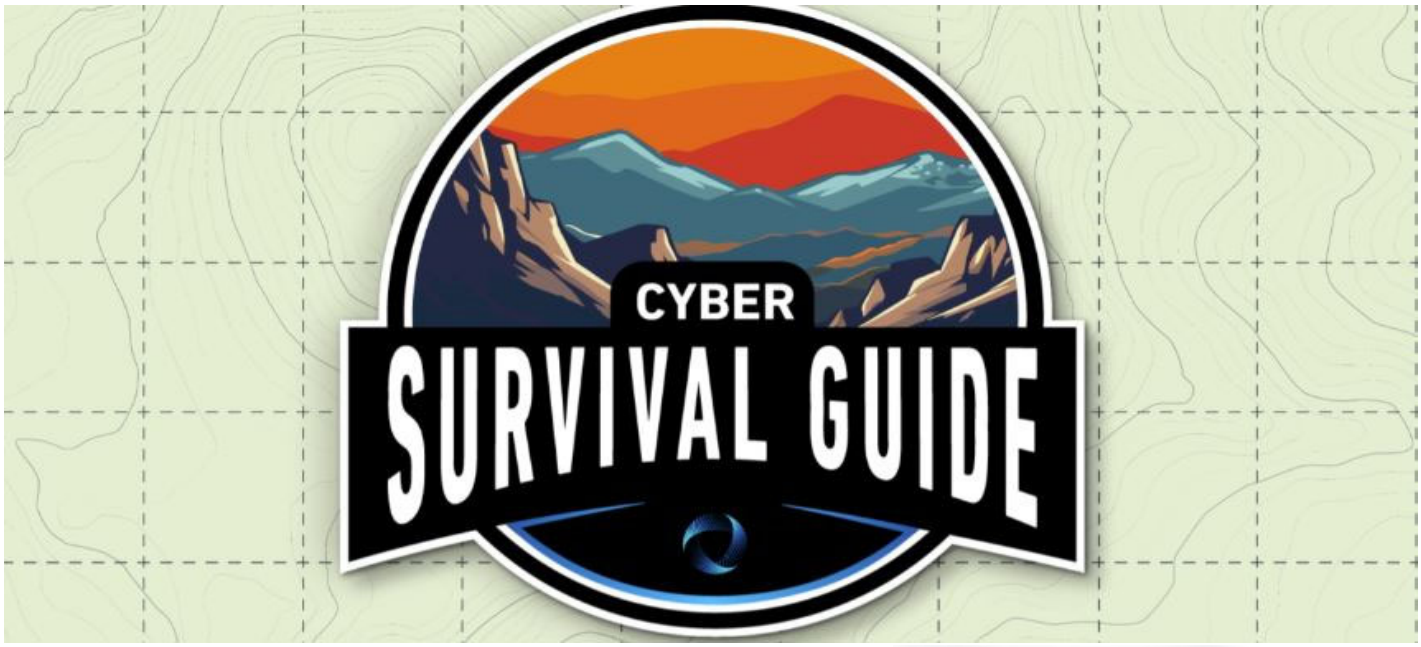
Dental Managers Society Newsletter
We Welcome Medical Managers!
August 2024

The spirit of adventure beckons you online!

You have funny GIFs to find, emails to ignore, pants to buy. But perils lurk in the dark corners of the web. Even when you try to maintain good habits, you can encounter packs of cybercriminals and malicious software..

What is there to do? Don't despair! We're here to help! Use the following as a survival guide for when you think you downloaded a virus, when you suspect an online account has been hacked, you've lost control of a social media account, your sensitive data was lost in a data breach, or a cybercriminal is threatening you with ransomware.



Stay safe online by being prepared

As with most things, preventing a cyberattack is easier than dealing with the fallout in many cases. By practicing some good cyber hygiene behaviors, you can stay on the trail headed to amazing internet experiences!

Remember, with all these situations, the most common way hackers get access to your private digital life is through phishing – no, not the kind at a lake. Keeping calm and collected when a suspicious message slithers into your inbox helps stop a hacking attempt before the hook is set.

How to Survive a Hacked Account

Fearless internet explorers, you can reclaim online accounts even if a hacker sneaks in! With some quick, sure-footed action, shoo cybercriminals out of your social media, email, or other

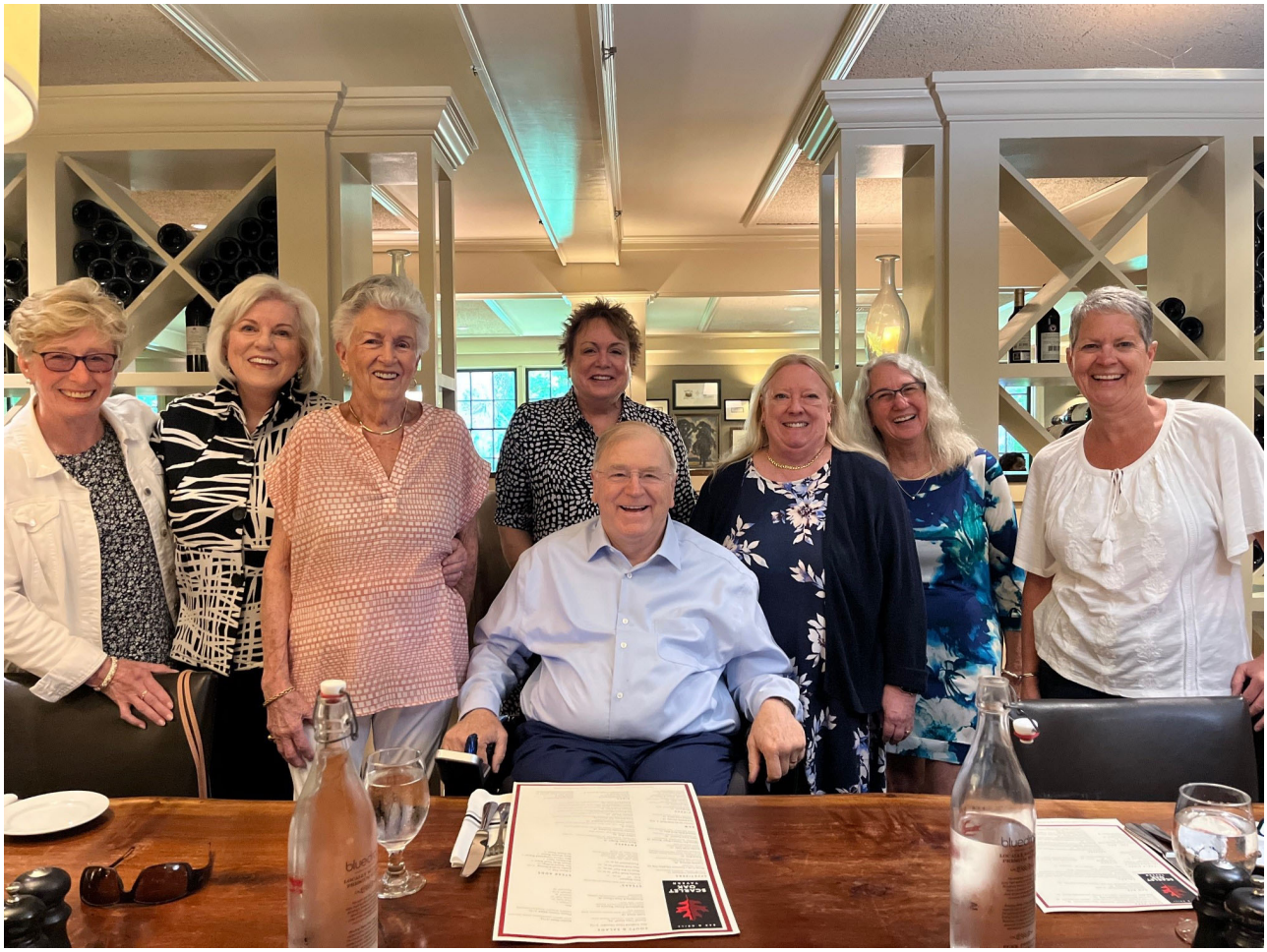
Continued on page 3

Letter from the Editor

Pam Snell,
DMS Advocate

Last month, we lost our dear friend and mentor Dr. Barry Brodil. We worked for Barry at Creating Ultimate Smiles in Hanover for over 20 years. During that time, he gave us the opportunities to learn and grow, something that we have never forgotten.

At his wake, people waited in line over an hour or more. Every one had a "Barry story" to tell. Those of us who lingered were able to also enjoy and reminiscence with others.



The next day, it was truly a Celebration of Barry's Life! Even though we thought we knew him well, we heard about more wonderful acts of kindness, wise counsel, and compassion.

As one person said, "When we think of Barry, we see his smile, his sense of humor, his energy and enthusiasm for life, and his love of adventure and people. He will be missed by all who knew him."

Barry, we love you!

Pam & David

(or several) of your accounts have been compromised and how you can restore order to your online basecamp.

Look out for telltale signs that your account has been hacked. There are a few common signs that an online account has been compromised:
• Your social media profile publishes posts that you didn't create.
• Your account sends phishing emails or DMs to others that encourage them to click on a link, download an app, or buy something.
• Friends and followers tell you that they've received emails or messages that you never sent.
• A company alerts you that your account information was lost or stolen in a data breach.

Change the account's password right away. You can lock out a cybercriminal by changing the account's password. Unfortunately, this also works the other way around: the hacker might change the password to lock you out. If this happens, use the account's "Forgot my Password" function to reset it. If more help is needed, contact the online platform or website ASAP about the situation.

Notify your contacts that your account was hacked and that they might receive spam messages that look like they came from you. Instruct your friends, family, colleagues, followers, and other contacts not to open these messages or click on any links contained in them. When the situation is cleared up, let everyone know your accounts are secure again.

Get help. If you suspect someone has stolen money from you, contact your bank and the local police. If a work account was compromised, contact your company's IT department. If you think your identity was stolen, contact the three credit bureaus and the FTC. Contact the respective online platform regarding the hacked account. Contact trusted friends and family about the matter so they can be on the lookout for weird communications from your online profiles.

How to Survive Losing Control of a Social Media Account

For many of us online, social media is how we unzip our tent flaps and enjoy the beauty of the online world. Social media is how we communicate with friends and family (and remember their birthdays). For some of us, it is an integral part of our business. Losing control of a social media account is like annoying hacker mosquitos invading your digital tent! When a cybercriminal takes over your socials, they can pretend to be you online and have access to your sensitive personal data. If you've lost control of a social media account, here are our tips to get it back.

1. **Determine if you've truly lost control of the account.**

   Don't take any unexpected urgent message about a social media hack at face value, but it is something to investigate. Also, a friends might say that your profile is making posts or sending messages that seem strange, like posting about a deal on sunglasses. Try to log into your social media account. If you can, immediately do the following:
   • Reset your password, and make it unique to the account, at least 16 characters long, and a mix of letters, numbers, and symbols.
   • Enable multi-factor authentication, which adds a whole new level of security to your login beyond your password.
   • Report the incident to the platform – you can even use screenshots as evidence.

Continued on page 6

Avoiding Voting Scams and

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

Safeguarding Elections

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 – so 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/

other account, change those passwords. Start using a password manager to generate and store all of your special, extra-strength passwords.

1. **Contact the platform.**
   If you cannot log in to your account, you need the social media platform to help you.
   • See if you can report the account takeover through the platform's website.
   • Call the social media network's customer service line if they have one.
   • Follow instructions on the platform's "forgot my account" or "account recovery" webpage. If contacting the platform doesn't work initially, be persistent. Unfortunately, social media platforms aren't known for their customer support. Take screenshots of anything your hacked profile posts, or have your followers record evidence, so you can better explain the situation to the platform.

2. **Once you have your formerly hacked account back, contain the damage by changing your password and turning MFA on.**
Look up recent activity on your profile page and in the accounts settings:
• Delete anything posted or sent by the hacker after taking a record.
• See if privacy or security settings were changed and adjust them to your comfort level.
• Check to see what devices have logged into the account and make a record of anything suspicious.

Take records of everything through screenshots. You can send this evidence to the social media platform or law enforcement.

Let your audience know you were hacked, even if it is embarrassing. People understand, and it is the best way to staunch any reputational damage the hacker did to you. Let them know they should be suspicious of any weird messages or odd posts coming from your profile.

Finally, review any personal data that was stored in the social media account, like credit card numbers or private DM communications. That data was compromised, and you might want to take further steps, like contacting your credit card issuer to cancel your card.

Other Cyber Merit Badges Include:

How To Survive a Ransomware Attack

How To Survive a Data Breach

How To Survive a Computer Virus

How To Survive a Phishing Attempt

You will find the full guides to earn each of these Cyber Merit Badges at:

https://programs.staysafeonline.org/cyber-survival | ***https://www.ACTSmartIT.com/survival***

Our thanks to the Cyber Security Alliance for "Empowering a Safer Digital World"
www.StaySafeOnline.org

PLANNING AHEAD — Yes, in August

NOW is the time to think ahead regarding your policies and practices, rather than waiting until the end of the calendar year.

Many employers have traditionally chosen to issue performance reviews in December of each year. Such reviews, if positive, are usually accompanied by a raise and/or bonus. On the other hand, if the review reflects performance that is unsatisfactory, that leaves the business entity in a bit of a quandary. What does one say? "You're not meeting expectations, so we're not giving you a raise or bonus. Happy Holidays."

A better HR practice would be to conduct performance reviews at the end of September or beginning of October. If an employee is underperforming, that allows the business to consider issuing a performance improvement plan. The timing provides the employee with the ability to work on specific areas that are deficient. A fall review also presents an opportunity to discuss possible coursework or certifications for which the employee can enroll, making this a "goal" for the coming year.

An employer, while writing up a review in August or September, may unfortunately realize that an employee is underperforming or is not a "good fit" and is one that the company does not wish to rehabilitate or retain. Addressing the need to terminate an employee can be done in a more thoughtful and time appropriate manner in the fall and this alleviates the pressures of a company having to deal with a reorganization, advertising for a new employee, or making major staffing changes at the very end of the year.

In addition, this is also a preferable time to revise old handbooks or create new policies. Moreover, it may be more convenient to schedule annual anti-harassment training sessions during this time as well. Think about getting these programs done before the period from Thanksgiving through the New Year, when many employees are utilizing PTO.

They say that timing in life is everything. That definitely applies to best practices in the workplace.

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

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:

- **Cyber Survival Guide**
- **Avoiding Voting Scams and Safeguarding Elections**
- **Planning Ahead—Yes, In August (Your HR Policies and Practices)**
- **And More**

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
508 272-5120
SusanR@GrammarGoddess.com