LI People ON THE MOVE

newsday.com/onthemove

ORSTED

Amy Ellis, of Mount Sinai, has been hired as stakeholder relations manager for New York at **Orsted** in Manhattan. Ellis was a senior specialist, government affairs and community relations for offshore wind, at Eversource Energy in Manhattan.

JPMORGAN CHASE

Alan Petrilli, of Glen Head, metro New York market executive for middle market banking and specialized industries and national apparel industry lead at **JPMorgan Chase** in Melville, has been promoted to Long Island region manager for middle market banking and specialized industries and national apparel industry lead.

J.P. MORGAN PRIVATE BANK

Donna Dougan, of Greenvale, has been hired as executive director and banker at **J.P. Morgan Private Bank** in Greenvale. Dougan was a private client relationship manager at TD Bank in Manhattan.

HOSPITAL FOR SPECIAL SURGERY

Dr. **Matthew Sikina**, of Port Washington, has been hired as a sports medicine physician at **HSS Long Island** in Uniondale. Sikina was a sports medicine fellow at Stanford Health Care in San Jose, Calif.

NY VINTAGE CAM

Dr. **Joe Verghese**, of Port Jefferson, has been hired as chair of the department of neurology at the **Renaissance School of Medicine at Stony Brook University** in Stony Brook. Verghese was a professor of neurology at Albert Einstein College of Medicine in Manhattan.

SID JACOBSON JCC

Robin Salsberg, of Merrick, has been hired as director of people and culture at **Sid Jacobson JCC** in East Hills. Salsberg was director, people and culture at New York Spine Institute in Westbury.

— DIANE DANIELS

Send submissions and color headshots to peopleonthemove@newsday.com

THE ISSUE: ONLINE FRAUD

Any business can fall prey to imitation scams

MONEY FIX

NerdWallet

The Federal Trade Commission received more than 330,000 reports of scammers impersonating businesses in 2023.

Some of these scammers pretend to be major corporations like Amazon or Best Buy, the FTC says. But small businesses are at risk too, says Scott Taber, a cybersecurity awareness program specialist at the Michigan Small Business Development Center.

"There's always been this idea that small businesses are too small. But we know that's not true — that cybercriminals specifically target small businesses because of that fact," Taber says. "Small businesses typically don't have the same resources as the larger organizations."

You can take steps to protect your business from fraudsters even without a dedicated risk or security team.

Here are some simple ways to spot and address imitation scams.

See if you're being imitated

Take a half-hour each day to perform "online hygiene" by searching for information about your business, suggests Melanie McGovern, director of public relations and social media at the Better Business Bureau. That can help you notice anything unusual.

For instance, McGovern says, even businesses that don't have websites may be listed in third-party directories. Scammers can find those directories — which usually include identifying details about your business, like its address — and create an online presence, then start making fraudulent sales.

"That's unfortunately how the scammers think," McGovern says. "That's an opportunity for them."

Monitoring financial records like your business credit reports can show potential issues as well. For example, Taber says, a scammer might try to open up new lines of credit or make large purchases in your name.

He recommends paying attention to customer feedback, too. If a customer gets a strange email or friend request and they report it to you, take time to investigate.

GETTY IMAGES / HOPEST

Even a one-person operation should take time to do "online hygiene" and help prevent the business from becoming the victim of an imitation scam.

How to handle a scam

The most common imitation scams reported to the FTC in 2023 included:

- Fake subscription renewals, like emails claiming that a certain subscription needs to be renewed. Even if a customer doesn't have a subscription to that service, they might click on the link seeking more information.
- Fake giveaways and discounts, in which scammers ask customers to send money to them to claim their offer.
- Fake package delivery problems, like a text claiming to be from the U.S. Postal Service informing the customer there was a problem and they need to pay a fee to resolve it.

If a scammer is imitating your business and customers need to be cautious, tell them what's going on and what you're doing to prevent it from happening again. This is especially important with your most essential clients with whom you need to preserve relationships.

"If you are knowing that there is an active scam with your business and you hide it or don't acknowledge it . . . you're going to lose customers and clients that way," Taber says. "Your business reputation is going to take a huge hit."

Next, report the scammer to the authorities. If they're posting on social media, report it to the social media platform and ask them to take down the post or shut down the account.

Preventing future fraud

Don't wait until a scammer targets your business to begin tightening your security and improving your digital marketing.

The business cybersecurity basics are essential, McGovern says. Set up two-factor authentication on all of your accounts and require your employees to change passwords regularly. To dodge phishing attempts, always double-check that emails and text messages claiming to be from your bank or a business partner are from a legitimate address or phone number before you respond or click links.

Beyond that, make sure your business has a website and a presence on whatever social platforms you use to communicate with customers. If there's an account you no longer use, keep an eye on it to ensure it's not taken over by a scammer, McGovern says.

Cybersecurity insurance can help protect your business finances if your information is compromised.