# Cybersecurity at Westmount:
## Working Together to Create a More Secure Environment

Sometimes the apparent ease of an undertaking belies the extensive planning that precedes it. "Making the trains run on time" requires exacting management and close collaboration.

At Westmount, we hold a similar view when it comes to protecting our clients and their assets. Our technology team is the group that makes the trains run on time, allowing our work with clients to proceed smoothly. Behind the scenes, this group of professionals performs vital work for our firm across many areas, including in cybersecurity and fraud prevention.

## Our Tech Team: Dedicated to Vigilance

We caught up with three members of Westmount's technology team—**Chris Werner,** Chief Operating/Compliance Officer, **Veronica Fotos,** Director of Technology, and **Carlos Anleo,** Systems Architect—to share some insights about the steps Westmount takes to protect client accounts and firm data.

Chris, Veronica, and Carlos also provided thoughtful strategies that we can all follow—employees and clients alike—to enhance our online security, not just at Westmount, but across all aspects of our digital lives.

## The Big Picture

From time immemorial, bad actors have tried to separate people from their money. Through most of history, these interactions have depended on proximity—unscrupulous people have needed to interact directly with their unsuspecting victims—or at least their physical banks or brokerage houses.

With the advent of the digital age, the scale of possible harm has broadened. Cybercrime is an activity that transcends national borders. And since the perpetrators are often manipulating actions from afar, their invisibility can compound the challenge of detection and deterrence.

"Virtually every company has experienced some kind of cyberfraud attempt," according to Artemis Global Security, a leading cybersecurity consultant. "In 2020, roughly 75% of organizations around the world reported experiencing a phishing attack. The other 25% either didn't know they had been targeted for cyberfraud—or wouldn't admit it."

**Phishing** is a form of fraud that seeks to solicit personal information, such as passwords or credit card numbers, through emails that appear to be legitimate, but are criminal in their intent. The section below provides definitions of phishing and other common cybercrimes.

## Common Cybersecurity Threats

Here are a few examples of the more prevalent threats that exist in the digital space today:

Wire Fraud: A federal crime in which a perpetrator uses an interstate communications device, such as email, texting, or telephone to defraud another person or party. Often, wire fraud can involve some form of social engineering, in which a bad actor impersonates a client or trusted family member pretending to have an urgent need to transfer funds.

Phishing: A type of fraud, typically carried out by email, that is designed to "hook" people into surrendering their personal financial information, such as passwords or credit card numbers, by posing as a reputable company or organization.

Virus: Computer code that is capable of copying itself and wreaking havoc by corrupting a computer system or destroying data.

Malware: A catch-all term for various malicious software, including viruses, adware, spyware, browser hijacking software, fake security software, and ransomware.

Spyware: Software that enables a perpetrator to obtain hidden information about another user's computer activities.

Ransomware: A type of malicious software designed to take over a computer system and its data, locking it down and encrypting it until a sum of money is paid as ransom for release.

## The Antidote

To anticipate and thwart cyber criminals, a robust industry has arisen at the intersection of technology and security, designed to stay ahead of these bad actors and their malicious schemes.

At Westmount, we appreciate the gravity of this threat and dedicate considerable resources to preemptively protect the integrity of client accounts and data. Our investment in digital security includes human capital—both our own team members and external experts—as well as technology, training, and education.

Below, you'll learn about our efforts to anticipate, detect, and thwart cybercrime in its various forms. We also encourage you to join us in embracing a few best practices to follow when it comes to your own security.

## Defense Wins Ballgames

If you've ever coached a sport, you may have heard people claim that "defense wins ballgames." We take a similar approach at Westmount when it comes to cybercrime, creating robust defenses to ward off possible attacks. Vigilance requires effective collaboration across our team members, vendors, and clients.

Here are a few of the measures we have put in place to create a more secure environment:

### Investment

The cybersecurity landscape is ever-changing. Staying current on the latest threats and their prevention requires significant investment in hardware and software. We commit substantial resources—both human and financial—to maintain a secure environment, recognizing that this investment is fundamental to our success (and that of our clients).

### Training

We conduct periodic training sessions for employees, led by one of the nation's pre-eminent cybersecurity experts. In these sessions, our team learns about the evolution of online threats and how to prepare for issues that may loom on the horizon. Our technology team also regularly shares their professional knowledge firmwide, conveying tips and news alerts throughout the year.

### Testing

We conduct annual due diligence on our vendors to ensure their technology, systems, and protocols are as robust as our own. We also regularly engage with experts to evaluate our systems and proactively rectify any possible areas of concern.

### Policy and Process

Cybercriminals have become more sophisticated in recent years, eschewing brute force-style assaults on computer systems for more insidious approaches, such as social engineering. Here, a criminal uses intimidation, flattery, or psychological manipulation to gain access to sensitive information, typically by interacting with another person who is oblivious to the criminal's intent. At Westmount, we work extensively with staff to educate them about the threat of social engineering and the disciplined processes to observe when such attacks are suspected.

## Positive Steps You Can Take

As the saying goes, "an ounce of prevention is worth a pound of cure." When it comes to cybercrime, this maxim proves its worth. There are some positive steps you can take to help mitigate the chance of being victimized by a cybercrime. Here are a few suggestions:

**Use unique, rigorous passwords** for each of your login sites. Do not reuse passwords from other accounts or across other sites.

**Employ 2-factor authentication,** known as 2FA, to verify your identity and gain access to your accounts. This process requires an additional login credential—often a code that is sent by text, email, or phone call. If you are a Westmount client, you already use 2FA to access your online statements and send or receive documents securely.

**Keep your anti-virus software up-to-date,** even if you use Apple products. Viruses can be malicious, no matter what operating system you use. Anti-virus software is your best line of defense.

**Suspicious links and attachments** are a potential source of harm. Only open those links and attachments that you are expecting, and only from sources you know and trust.

## If You Suspect a Breach

If you notice any suspicious activity with your account, please reach out to your Westmount Advisor right away.

Perpetrators of cybercrimes are becoming more and more sophisticated. By following these best practices, staying vigilant, and using common sense, we can greatly reduce our risk of falling victim to these schemes.

If you have any questions about Westmount's cybersecurity practices, please contact your advisor or email us at info@westmount.com.

## About Westmount

Westmount is one of L.A.'s leading independent investment firms.

One of the most satisfying aspects of the work we do is seeing the impact it has on our clients' lives. We've been honing our collaborative approach for more than 30 years, guiding clients through tumultuous markets and major life events along the way.

Our clients can count on us to do the research, create the plans, manage the portfolio, provide the counsel, and do whatever else is needed to help them achieve their financial goals. Our robust advisory platform encompasses a broad range of integrated services, including investment portfolio construction, retirement planning, tax strategies, insurance review, estate and legacy planning, and more.

For more information, call us at 310-556-2502 to speak with an advisor, or email info@westmount.com.

Copy by Katherine Doyle



If you have any comments or questions about this report, please contact us at info@westmount.com.

Westmount Asset Management, LLC
2049 Century Park East, Suite 2500 | Los Angeles, CA 90067 | Tel: 310-556-2502