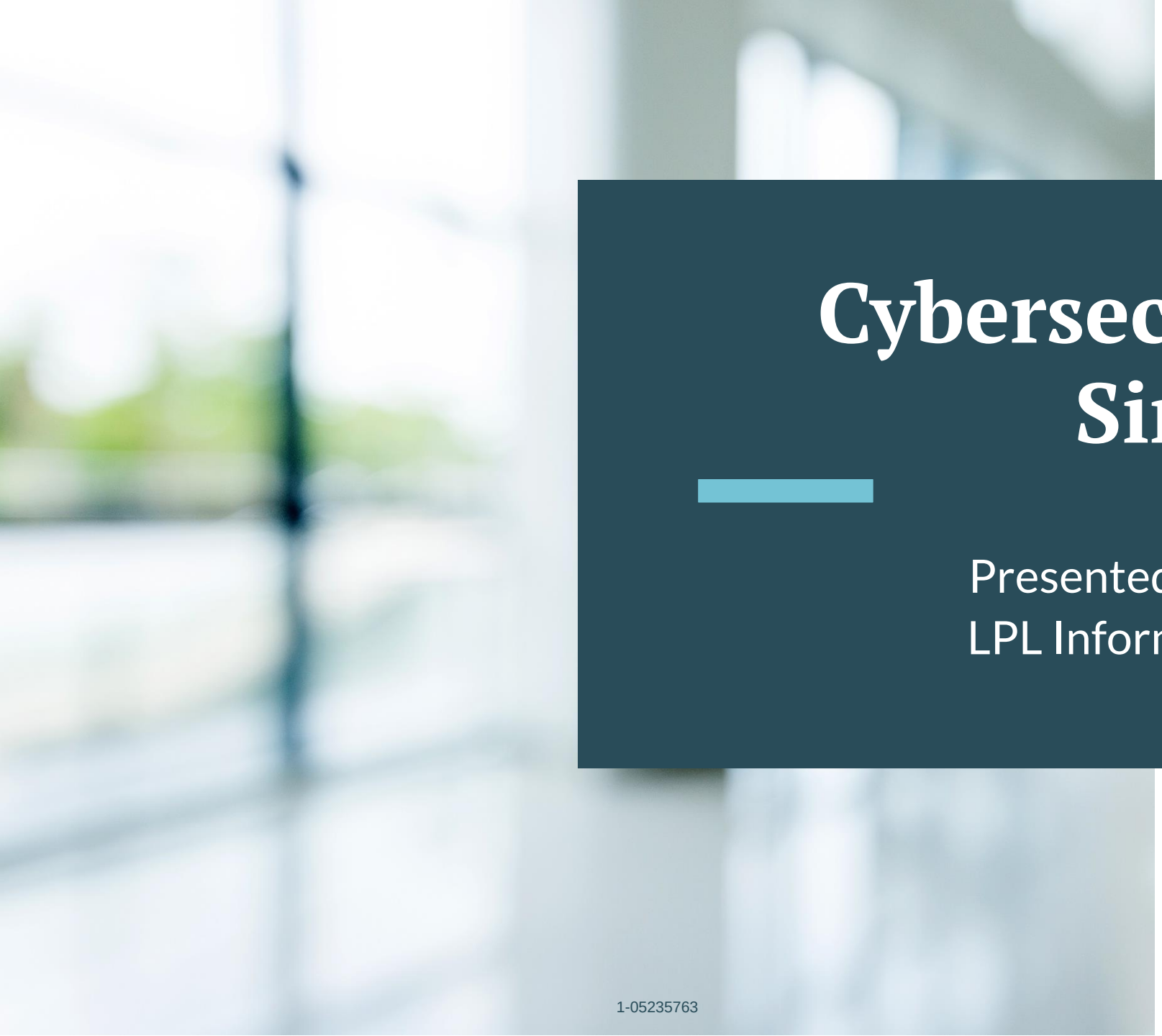


Cybersecurity Made Simple

Presented by Mike Terry
LPL Information Security

JOHNSON FINANCIAL GROUP® FINANCIAL ADVISORS

Today's Speaker

Mike Terry

Senior Analyst on Advisor Information Security Team

LPL Financial

Agenda

01 Protecting Your Information

02 Identifying Cyber-Attacks

03 Securing Your Information

04 Protecting Your Family

JOHNSON FINANCIAL GROUP® FINANCIAL ADVISORS

Protecting Your Information

Keeping your Information Safe

LPL is committed to protecting sensitive information

JOHNSON FINANCIAL GROUP®

#LPLProtected

YOU	Your Firm	LPL Financial
Investment account	Recurring trainings	Dedicated cyber staff
Assets	Personal relationship	State of the art facilities
Personal information	Secure financial tools	Cyber insurance

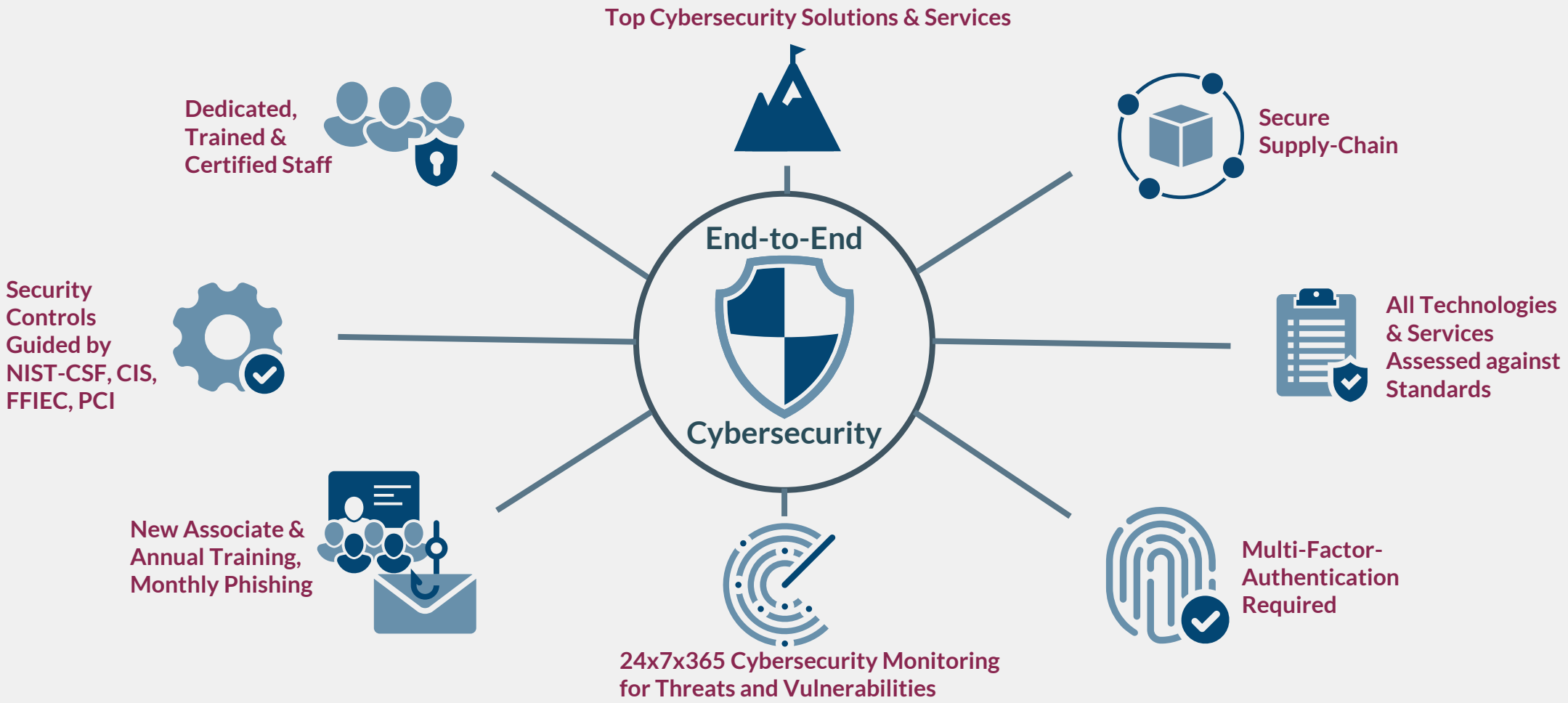
Cyber Fraud Guarantee

Visit LPL's cybersecurity page to learn more

"LPL will reimburse you for 100% of realized losses in your impacted LPL accounts, which were incurred directly as a result of unauthorized access to an LPL system."

Cybersecurity at JFG

Keeping your data and assets safe from Cybersecurity threats end-to-end



Cyber attacks

Identifying Cyber Attacks

Who and what are behind these attacks?

Hackers use computer networks to advance social and political causes.

Cybercriminals steal personal information and extort victims for financial gain.

Trusted insiders steal proprietary information for personal or financial reasons.

Nation-state actors steal state secrets and other proprietary information from private companies.

State and nation-state terrorists create fear and impact our safety by attacking critical computer systems.

Nation-state actors sabotage military and critical infrastructure systems to gain advantage in the event of war.

Identifying Cyber Attacks

Who and what are behind these attacks?

What is it?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Why should you care?

Bad actors are constantly evolving their tactics to access information in unauthorized manners. Once they've received access, they will use the information to commit fraud.

Cybercriminals

Hacktivism
Social or Political Interests

Crime
Extortion or Financial Gain

Angry Employees
Financial or Personal Gain

Espionage
Info or Intellectual Property

Terrorism
Create Fear or Harm

Warfare
Sabotage critical public or military infrastructure

Social Engineering

These attacks are designed to take advantage of human emotions

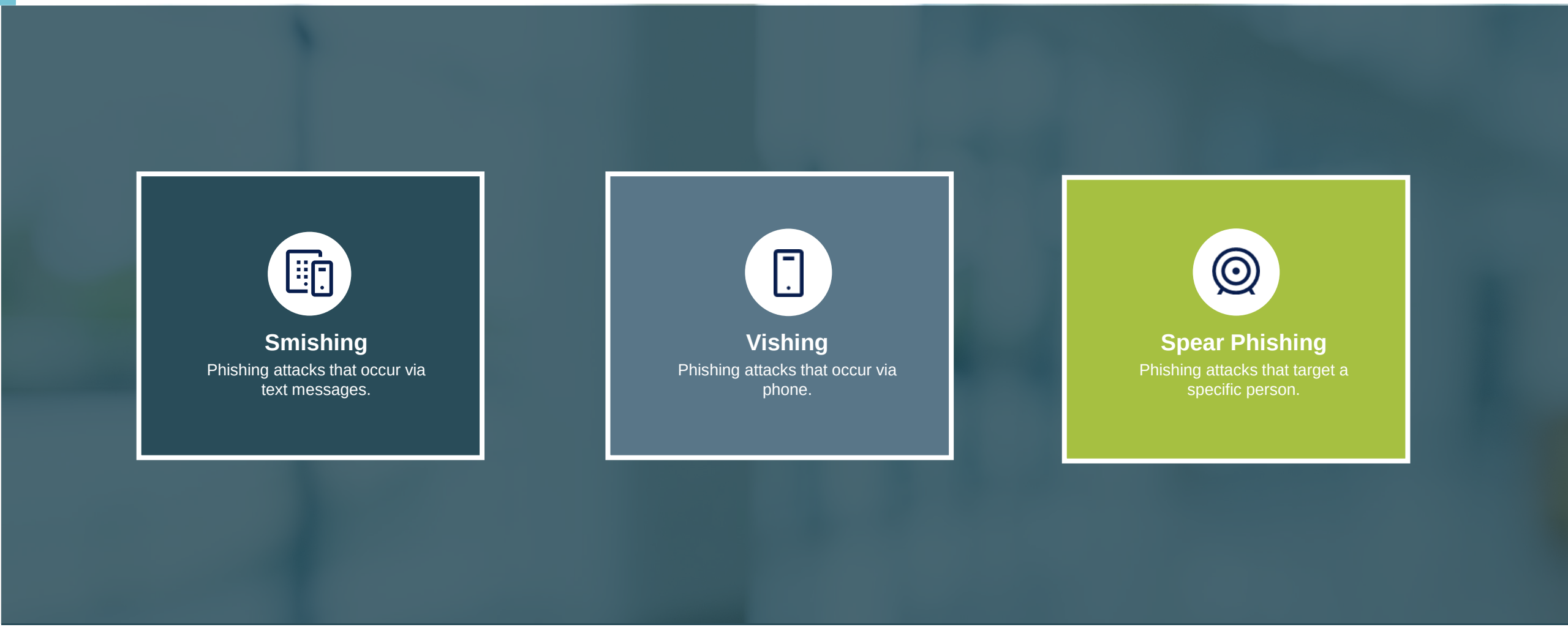
1. **Phishing – suspicious emails sent to large groups of individuals. The goal is to get the recipient to click a link or open attachments.**
2. **Ransomware – this malware or virus is often deployed after a link is clicked or attachment is opened in a phishing email.**
3. **Scams – Bad actors create realistic scams to trick unsuspecting individuals into exposing personal, financial, or corporate information.**
4. **Email Impersonations – An LPL client's email is compromised, and the bad actor does keyword searches to locate sensitive information.**

Identifying Red Flags in Emails

These attacks are designed to take advantage of human emotions

- Sense of urgency or an unusual request
- Unfamiliar tone to email
- Suspicious links or attachments
- Inconsistencies in email address, links and/or domain names

Additional Phishing Attacks



Smishing

Phishing attacks that occur via text messages.

Vishing

Phishing attacks that occur via phone.

Spear Phishing

Phishing attacks that target a specific person.

Avoiding Scams

Bad actors create realistic scams to commit fraud

Gift Card Scams

Investment Scams

Tech Support Scams

Invoice Scams

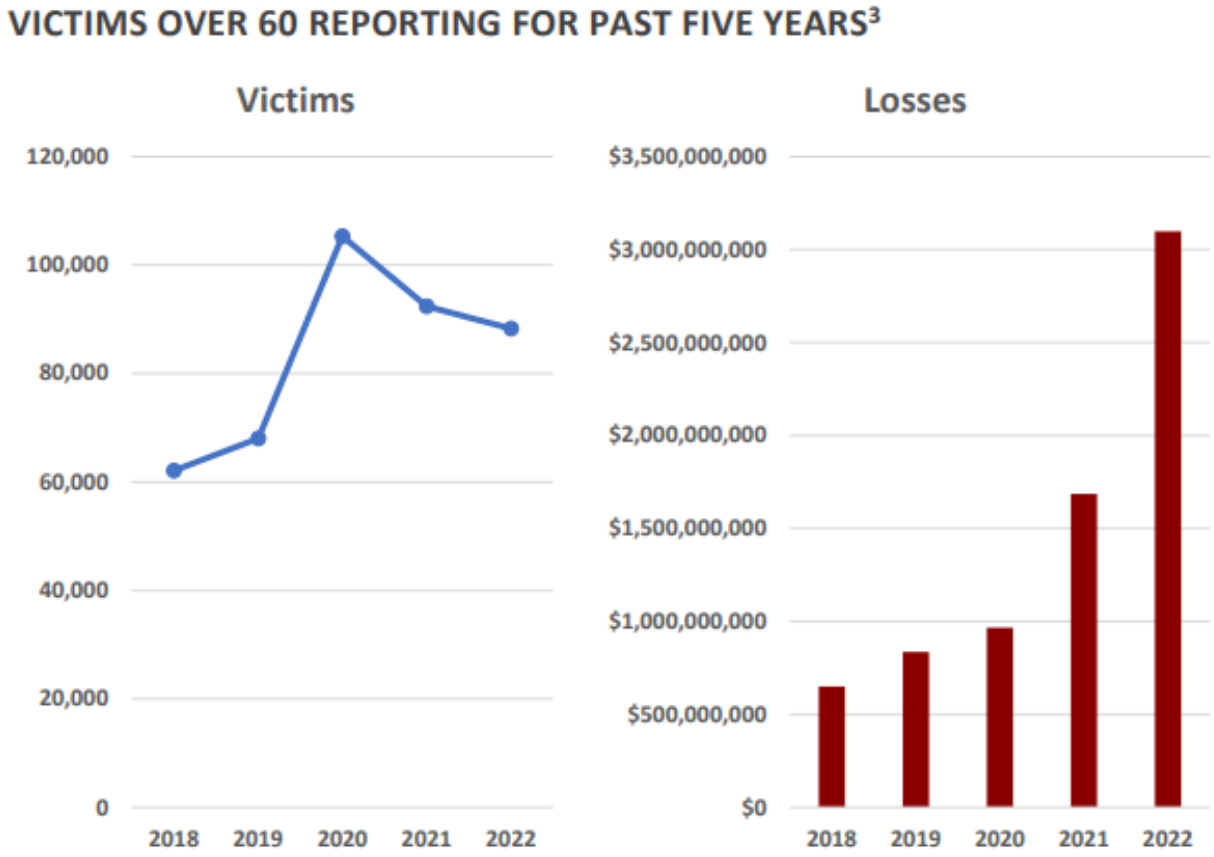
Elder Fraud

Examples of senior scams:

- Romance/Confidence
- Tech support
- Lottery/Sweepstakes
- Inheritance
- Identify Theft
- Government Impersonation
- Investment
- Healthcare

If you're unsure if your interaction is legitimate, immediately cease that interaction.

*Per Elder Fraud Report via the FBI



Customer Service/Tech Support scams impacted the most victims

What Do I Do Next?

These attacks are designed to take advantage of human emotions

1. **Change your passwords** – Phishing attacks often gain access to accounts and credentials. Always update your passwords and accounts if you are a victim of phishing.

2. **Check your accounts** – Be sure to monitor and check your accounts for unusual or unauthorized activity to accounts including banking, email, and social media.

3. **Notify JFG/IT** – Notifying LPL of an attack or compromise allows us to monitor your accounts and setup controls to protect your clients.

4. **Educate** – Education on phishing attacks is crucial to protecting your accounts. Adopting a proactive response to phishing attacks can save you many issues.

Securing Your Information

Password Security Tips

Prioritize length and complexity

Don't use personal information.
This can be publicly available & easily accessible by hackers.

Avoid using dictionary words.
Password-cracking tools can easily process every word in the dictionary.

Use multi-factor authentication (MFA or 2FA).
For especially sensitive accounts, enable and use MFA.

Don't re-use passwords.
If one account is breached, your others would be vulnerable as well.

Avoid typing passwords while using public Wi-Fi.
Use a VPN or avoid websites that require your login information.

Password managers are a convenient way to manage complex passwords over multiple platforms. Think of them as secure vaults that are great alternatives to reusing passwords.

Is Your Password Strong Enough?

How long would it take hackers to compromise your password?

Number of Character	Numbers Only	Lowercase letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 Secs	7 Secs	31 Secs
8	Instantly	Instantly	2 Mins	7 Mins	39 Mins
9	Instantly	10 Secs	1 Hour	7 Hours	2 Days
10	Instantly	4 Mins	3 Days	3 Weeks	5 Months
11	Instantly	2 Hours	5 Months	3 Years	34 Years
12	2 Secs	2 Days	24 Years	200 Years	3k Years
13	19 Secs	2 Months	1k Years	12k Years	202k Years
14	3 Mins	4 Years	64k Years	750k Years	16m Years
15	32 Mins	100 Years	3m Years	46m Years	1bn Years
16	5 Hours	3k Years	173m Years	3bn Years	92bn Years
17	2 Days	69k Years	9bn Years	179bn Years	7tn Years
18	3 Weeks	2m Years	467bn Years	11tn Years	438tn Years

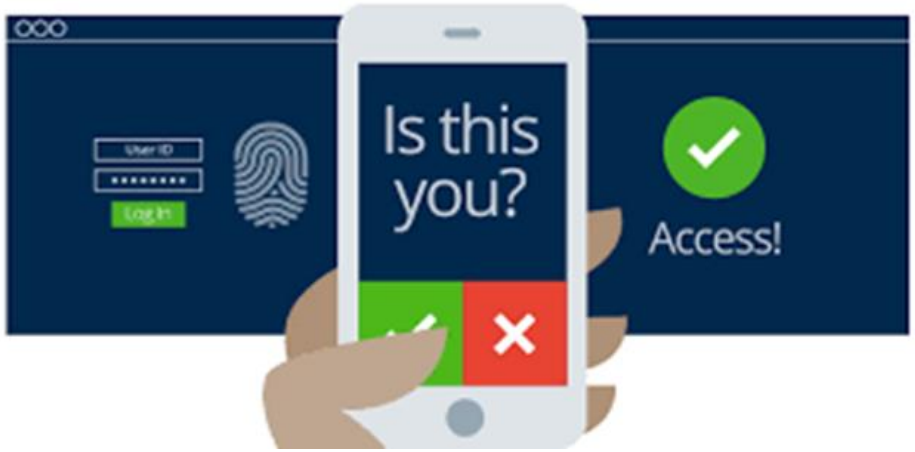
Multi-Factor Authentication (MFA or 2FA)

Using MFA adds an additional layer of security to your accounts.

What is MFA?

MFA is an authentication method that requires you to complete two methods of verification to gain access to an application.

.



If credentials are compromised, your accounts are still protected from unauthorized access.

Mobile Device Security

How safe if your device?

01 Add password and biometrics to your device.

02 Update mobile security software regularly

03 Only download known and trusted apps

04 Review app permissions

Protecting Your Family

Traveling safe

Stay Vigilant

1.

- Always be aware of your surroundings
- Never leave equipment unattended in public places.
- Learn about local scams

Use a Portable Charger

2.

- Avoid risks associated with public USB charging ports
- Portable chargers allow you to conveniently charge devices while traveling.

Protect Your Accounts

3.

- Enable MFA on accounts
- Review accounts for unauthorized activity.
- Avoid public Wi-Fi without using a VPN or hot-spot

Internet Best Practices

The misuse of the internet can lead to increased risks from cyber threats.

- Use strong passwords and turn on MFA
- Visit websites that URL start with https
- Use credit cards or third-party apps for payments
- Update your software

1-05235763

Securing Your Home

If you connect it, protect it.

Internet of Things

Best Practices

- Update software regularly
- Change default passwords to strong, complex passwords
- Use a password manager
- Enable MFA
- Opt-out of data tracking

Any device that has a sensor and is connected to the internet is an IOT

Protecting Your Identity

Make keeping your personal information safe a priority.

Protecting Your Family

The use of technology to harass, threaten, or target a person is called cyberbullying

Call to Action!

1. LPL is committed to supporting JFG and protecting your information.
2. Social engineering attacks take advantage of your emotions
3. Don’t click on links or open attachments from unknown sources.
4. Value security over convenience when traveling.
5. Protect your accounts and protect your family.

JOHNSON FINANCIAL GROUP®

FINANCIAL ADVISORS

1-05235763

Thank You

Securities and advisory services are offered through LPL Financial (LPL), a registered investment advisor and broker-dealer (member FINRA/SIPC). Insurance products are offered through LPL or its licensed affiliates. Johnson Financial Group and Johnson Financial Group Financial Advisors **are not** registered as a broker-dealer or investment advisor. Registered representatives of LPL offer products and services using Johnson Financial Group Financial Advisors, and may also be employees of Johnson Financial Group. These products and services are being offered through LPL or its affiliates, which are separate entities from, and not affiliates of, Johnson Financial Group and Johnson Financial Group Financial Advisors. Securities and insurance offered through LPL or its affiliates are:

NOT INSURED BY FDIC OR ANY OTHER GOVERNMENT AGENCY		
NOT BANK GUARANTEED	NOT BANK DEPOSITS OR OBLIGATIONS	MAY LOSE VALUE

JohnsonFinancialGroup.com

JOHNSON FINANCIAL GROUP® FINANCIAL ADVISORS

1-05235763