Cybersecurity Made Simple

Presented by LPL Information Security

JOHNSON FINANCIAL GROUP® FINANCIAL ADVISORS

Today’s Speakers

Mike Terry

Senior Analyst on Advisor Information Security Team

LPL Financial

Olivia Lack

Analyst on Advisor Information Security Team

LPL Financial

Madison Carroll

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

Questions During the Webinar?

Please email us:

JFGFASupport@johnsonfinancialgroup.com

Or

Contact your advisor

Protecting Your Information

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

Keeping your Information Safe

LPL is committed to protecting sensitive information

JOHNSON FINANCIAL GROUP® FINANCIAL ADVISORS

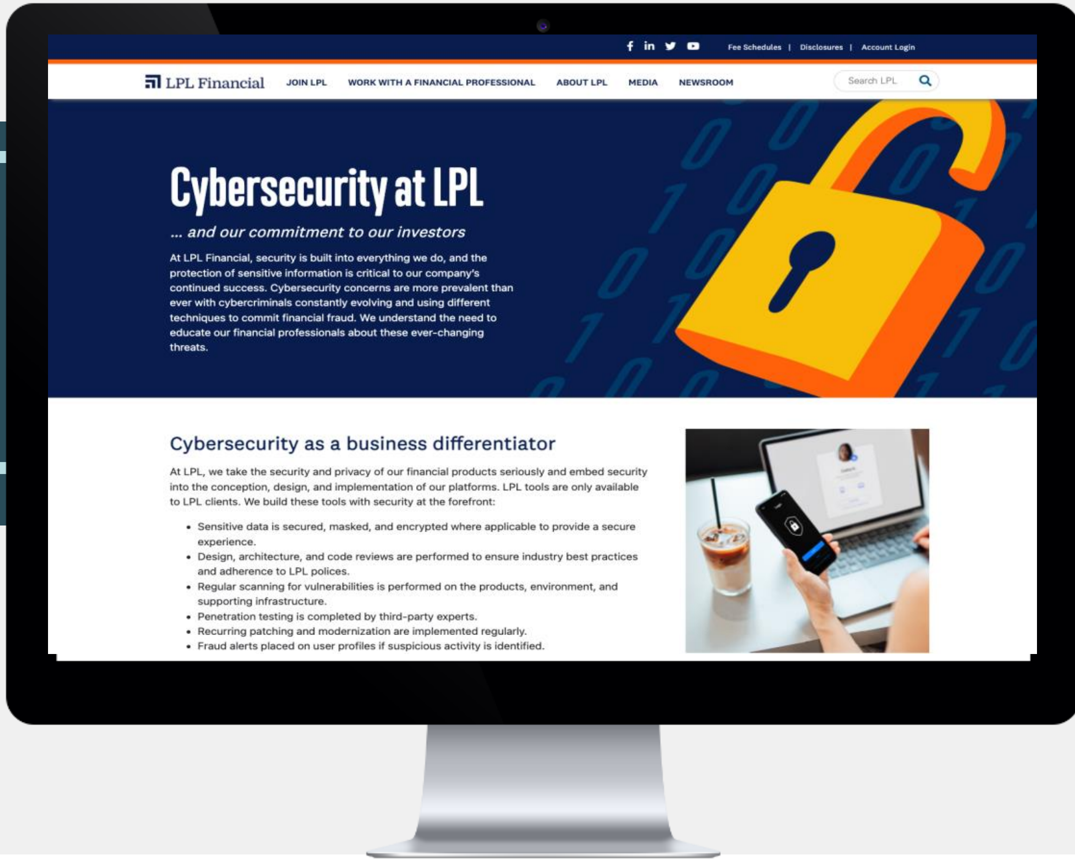
#LPLProtected

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."**


Fee Schedules | Disclosures | Account Login
LPL Financial
JOIN LPL
WORK WITH A FINANCIAL PROFESSIONAL
ABOUT LPL
MEDIA
NEWSROOM
Search LPL

Cybersecurity at LPL

... and our commitment to our investors

At LPL Financial, security is built into everything we do, and the protection of sensitive information is critical to our company's continued success. Cybersecurity concerns are more prevalent than ever with cybercriminals constantly evolving and using different techniques to commit financial fraud. We understand the need to educate our financial professionals about these ever-changing threats.

Cybersecurity as a business differentiator

At LPL, we take the security and privacy of our financial products seriously and embed security into the conception, design, and implementation of our platforms. LPL tools are only available to LPL clients. We build these tools with security at the forefront:

- Sensitive data is secured, masked, and encrypted where applicable to provide a secure experience.
- Design, architecture, and code reviews are performed to ensure industry best practices and adherence to LPL polices.
- Regular scanning for vulnerabilities is performed on the products, environment, and supporting infrastructure.
- Penetration testing is completed by third-party experts.
- Recurring patching and modernization are implemented regularly.
- Fraud alerts placed on user profiles if suspicious activity is identified.

Cyber attacks

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

Phishing scams

Smishing

Vishing

Quishing

Smishing

Vishing

Quishing

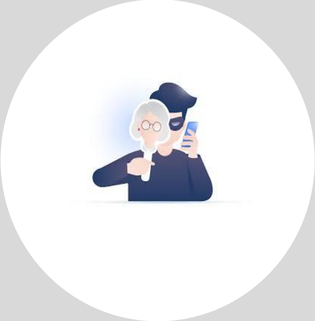
Vishing

Smishing

Quishing

Smishing

Vishing



Quishing

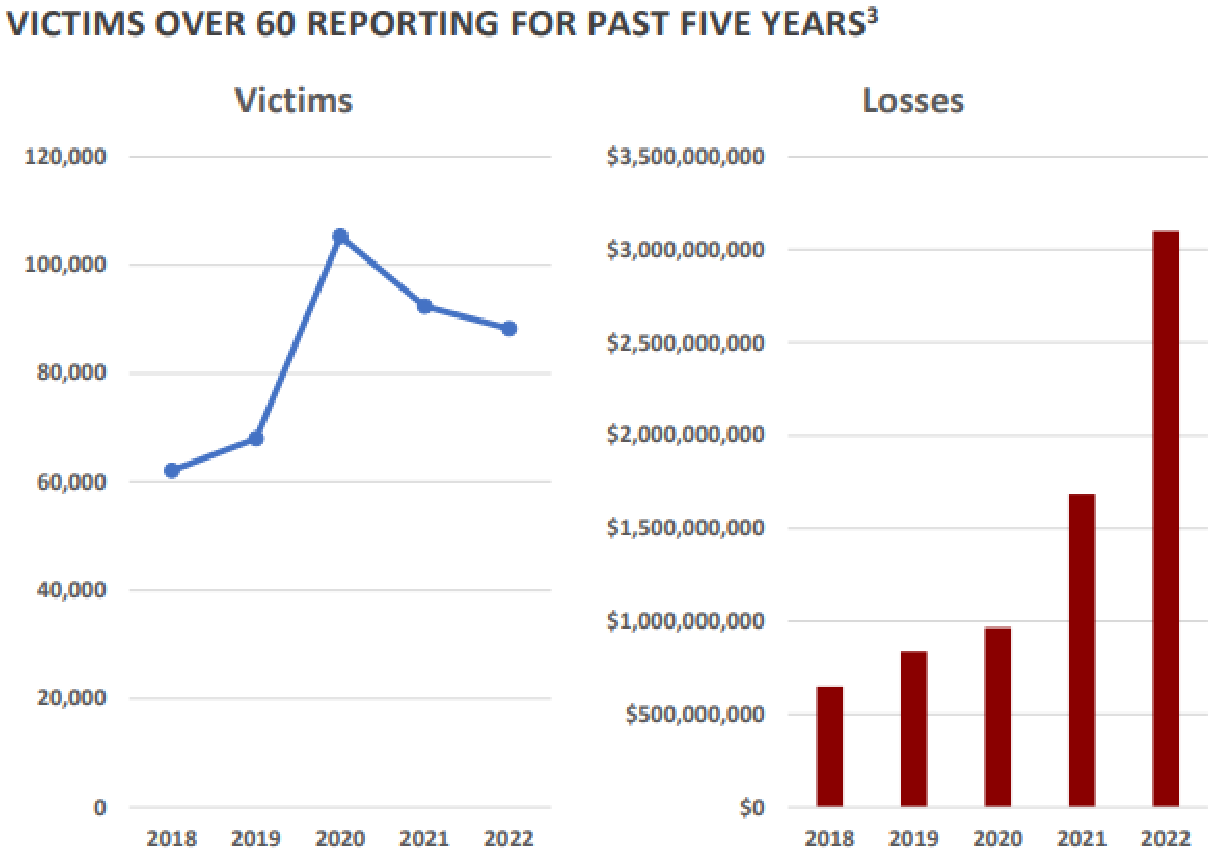
Elder Fraud

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



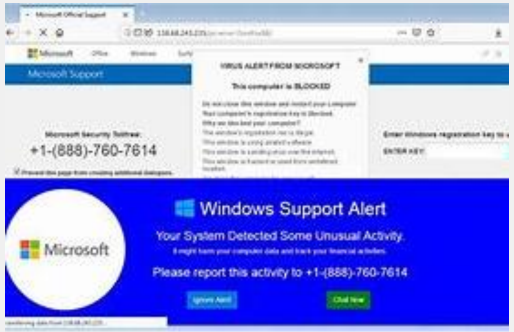
VICTIMS OVER 60 REPORTING FOR PAST FIVE YEARS[3]

Customer Service/Tech Support scams impacted the most victims

Avoiding Scams

Bad actors create realistic scams to commit fraud

Investment Scams



VIRUS ALERT FROM MICROSOFT

This computer is BLOCKED

Do not close this window and restart your computer
Your computer's registration key is Blocked.
Why we blocked your computer?
The window's registration key is illegal.
This window is using pirated software.
This window is sending virus over the internet.
This window is hacked or used from undefined location.

Microsoft Security Tollfree:
+1-(888)-760-7614

Enter Windows registration key to
ENTER KEY:

Windows Support Alert

Your System Detected Some Unusual Activity.
It might harm your computer data and track your financial activities.

Please report this activity to +1-(888)-760-7614

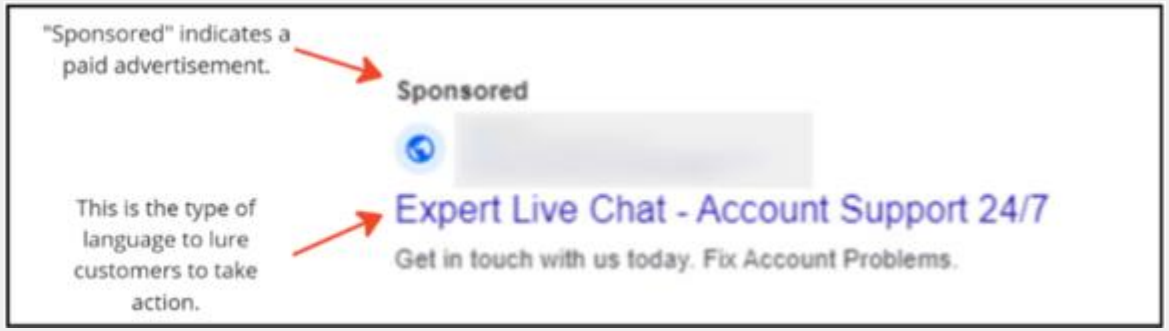
Tech Support Scams

Invoice Scams

Sponsored Ad Scams

Tips to Avoid Sponsored Ad Scams:

1. Avoid clicking on “sponsored” or “unsponsored” ads that appear via search results online.
2. Go directly to a company’s website to obtain reliable information.
3. Thoroughly review any website before entering sensitive information.



"Sponsored" indicates a paid advertisement.

This is the type of language to lure customers to take action.

Sponsored

Expert Live Chat - Account Support 24/7

Get in touch with us today. Fix Account Problems.

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?

Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	28 secs	2 mins	5 mins
10	Instantly	1 mins	21 hours	5 days	2 weeks
12	1 secs	14 hours	6 years	53 years	226 years
14	52 secs	1 year	17k years	202k years	1m years
16	1 hours	713 years	46m years	779m years	5bn years
18	6 days	481k years	126bn years	2tn years	26tn years

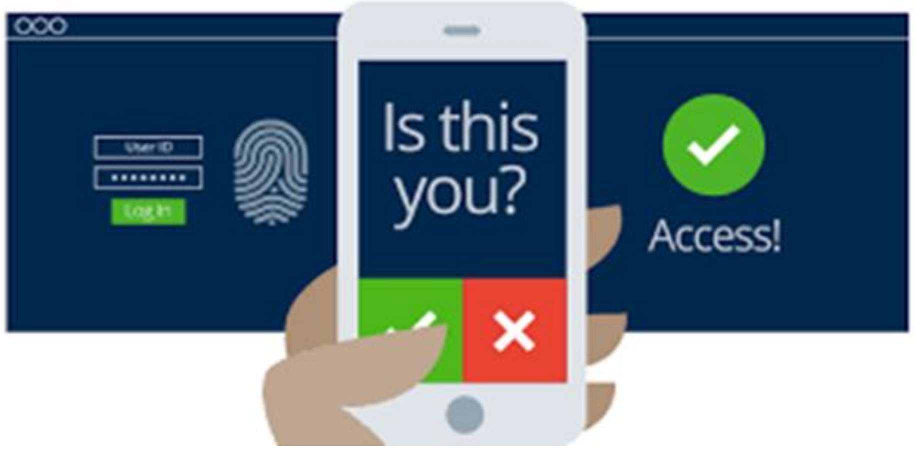
Multi-Factor Authentication (MFA or 2FA)

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 device software regularly

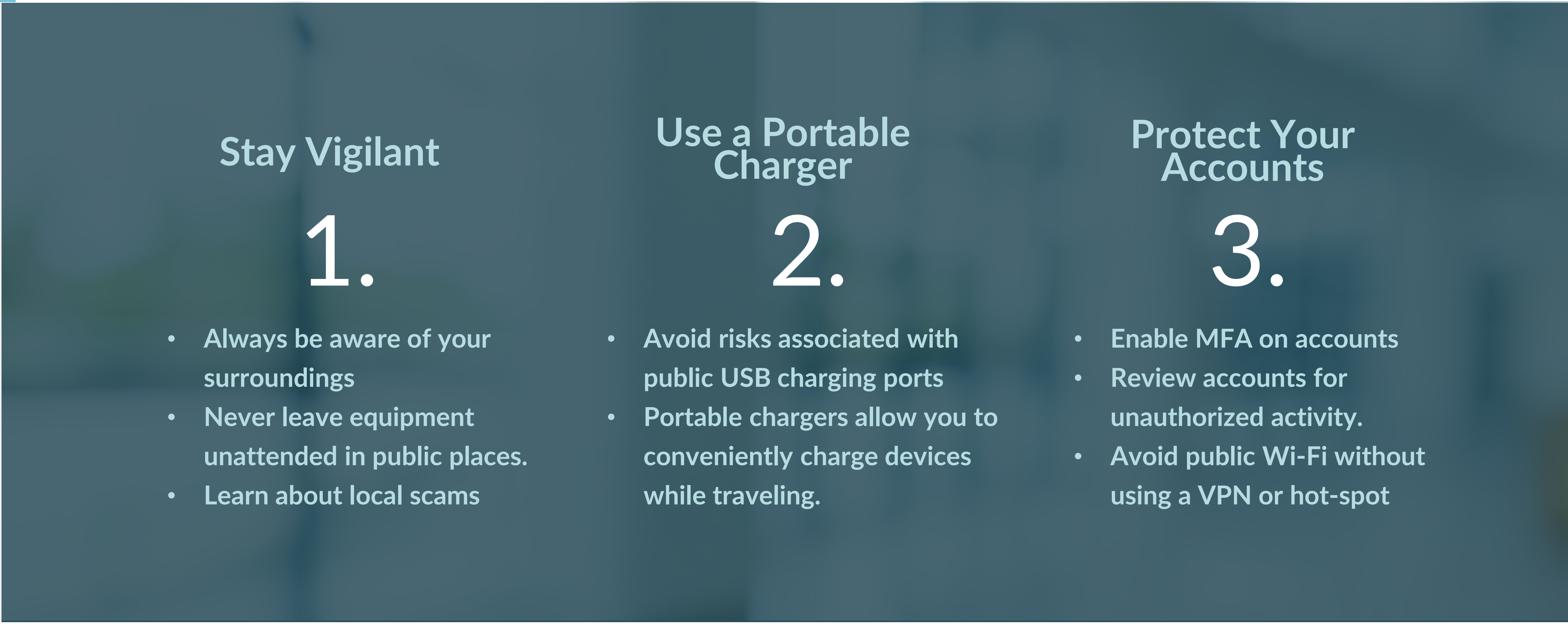
03 Only download known and trusted apps

04 Review app permissions

1-05235763

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.

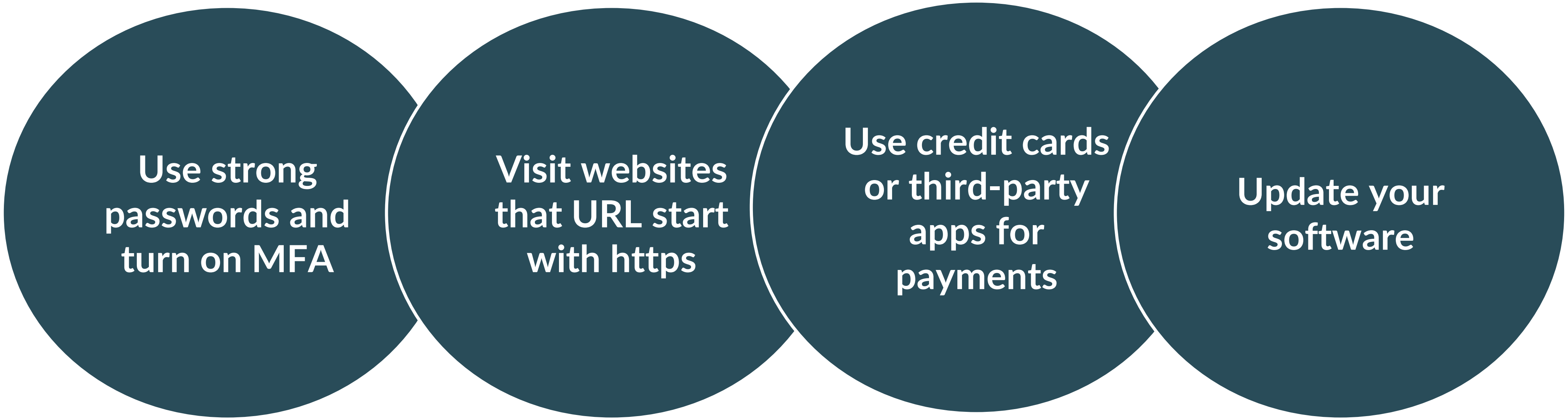
Protect Your Accounts

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

Securing Your Home

If you connect it, protect it.

Internet of Things

IoT
Auto Vac
SUPER COMPUTER

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

What is Artificial Intelligence (AI)?

Artificial Intelligence

AI involves techniques that equip computers to emulate human behavior, enabling them to learn, make decisions, recognize patterns, and solve complex problems in a manner akin to human intelligence.

Machine Learning

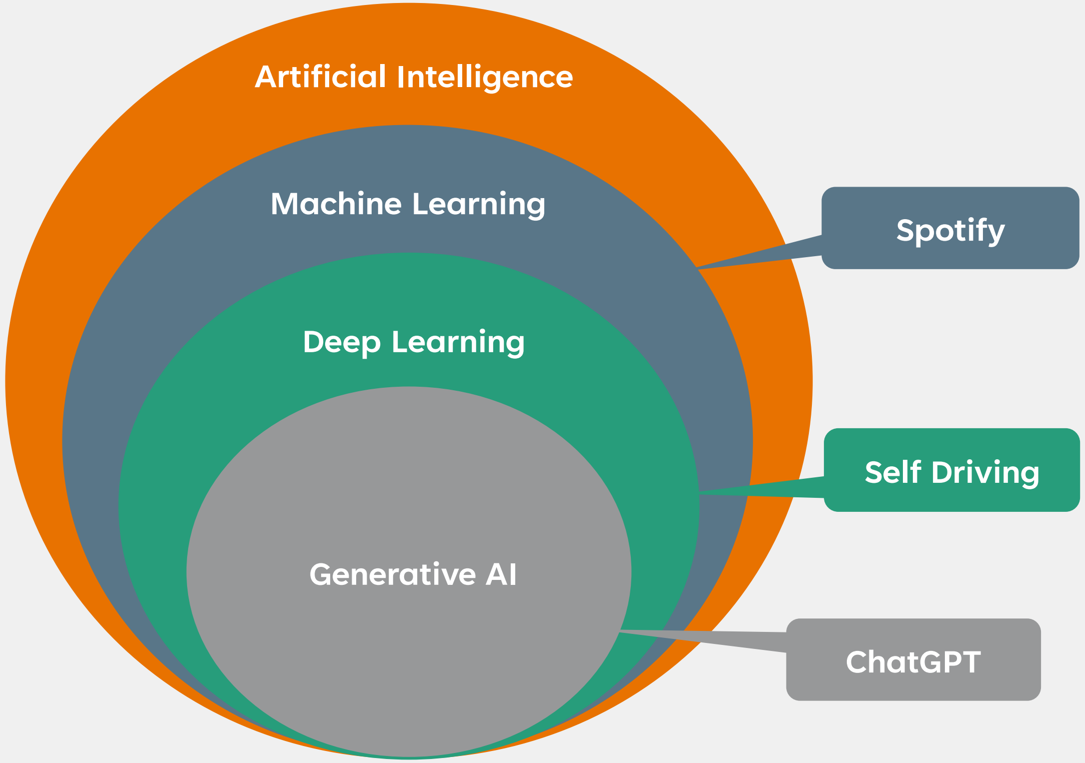
ML uses advance algorithms to detect pattens in large data sets, allowing machines to learn and adapt. ML algorithms use supervised and unsupervised learning methods.

Deep Learning

DL uses neural networks for in-depth data processing and analytical tasks. DL leverages multiple layers of artificial neural networks to extract high-level features from raw input data, simulating the way human brains perceive and understand the world.

Generative AI

“Gen AI” creates content like text, images or code based on provided input. Trained on vast data sets, these models detect patterns and create outputs without explicit instruction, using a mix of supervised and unsupervised learning.



LPL Financial

Do's and Don'ts of Generative AI

How to leverage the latest technologies safely

Understand the Limitations

Language models all have different training data that powers what it is adept and responding to. It is important to know what those limitations are before relying on it for research or additional insights.

Never Enter Private Information

Language Models like ChatGPT train on conversations that take place on their platform, entering private information is no different than voluntarily exposing the sensitive data entered.

Verify All Responses

AI can often generate information that is missing or misunderstood the context of what you are asking. Always read and assess the output of your request to ensure that it aligns with your initial request.

Never Assume AI is Correct

AI continues to have issues hallucinating information. Be sure to check sources and validate any information crucial to the output

Provide Clear & Specific Inputs

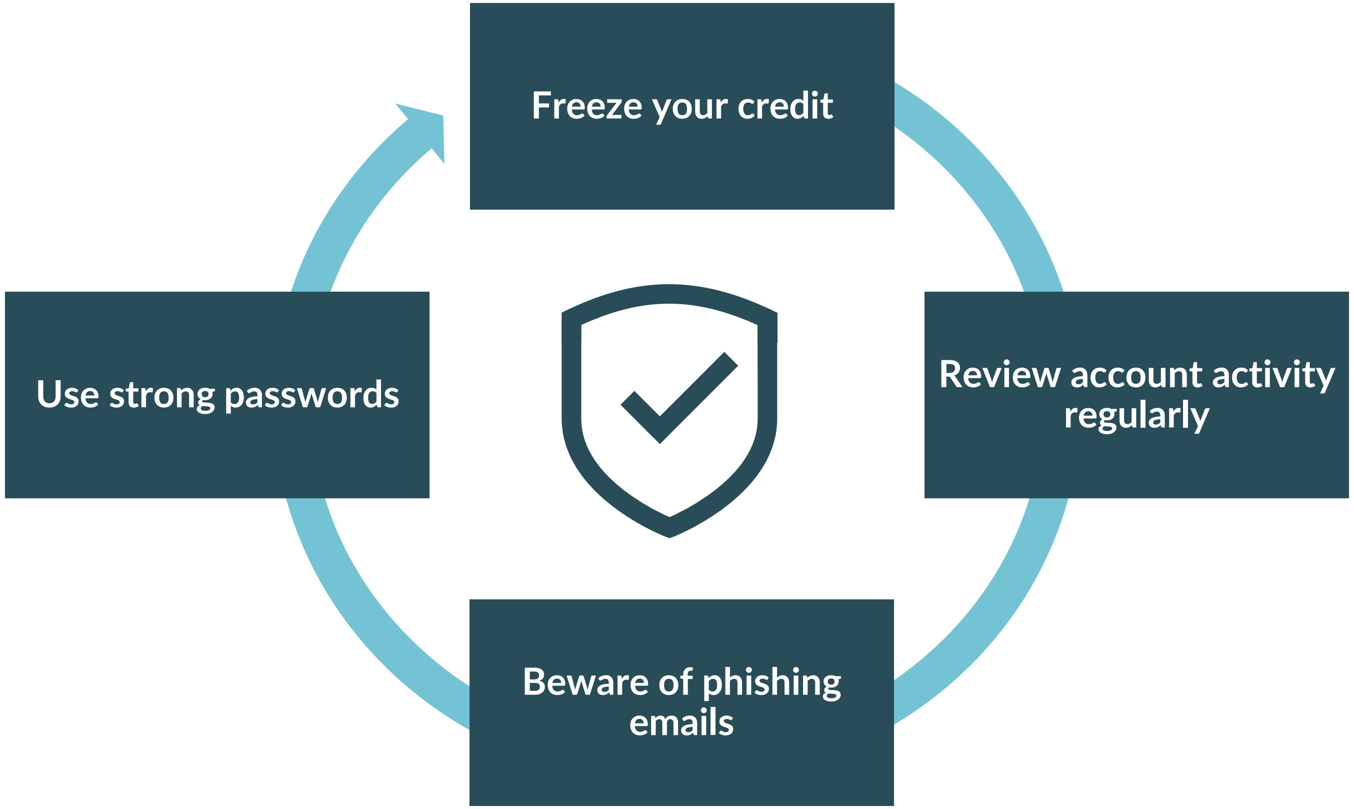
Provide accurate and relevant information when making a request. Context, Clarity, Examples, and Formatting are all important details that should be considered when leveraging an LLM

Never Use 3rd Party LLM Apps

When considering third-party language models like ChatGPT, ensure they have strong security and privacy measures before using them in your business. Follow the vendor management best practices enforced in the BOSP.

Protecting Your Identity

Make keeping your personal information safe a priority.



Freeze your credit

Review account activity regularly

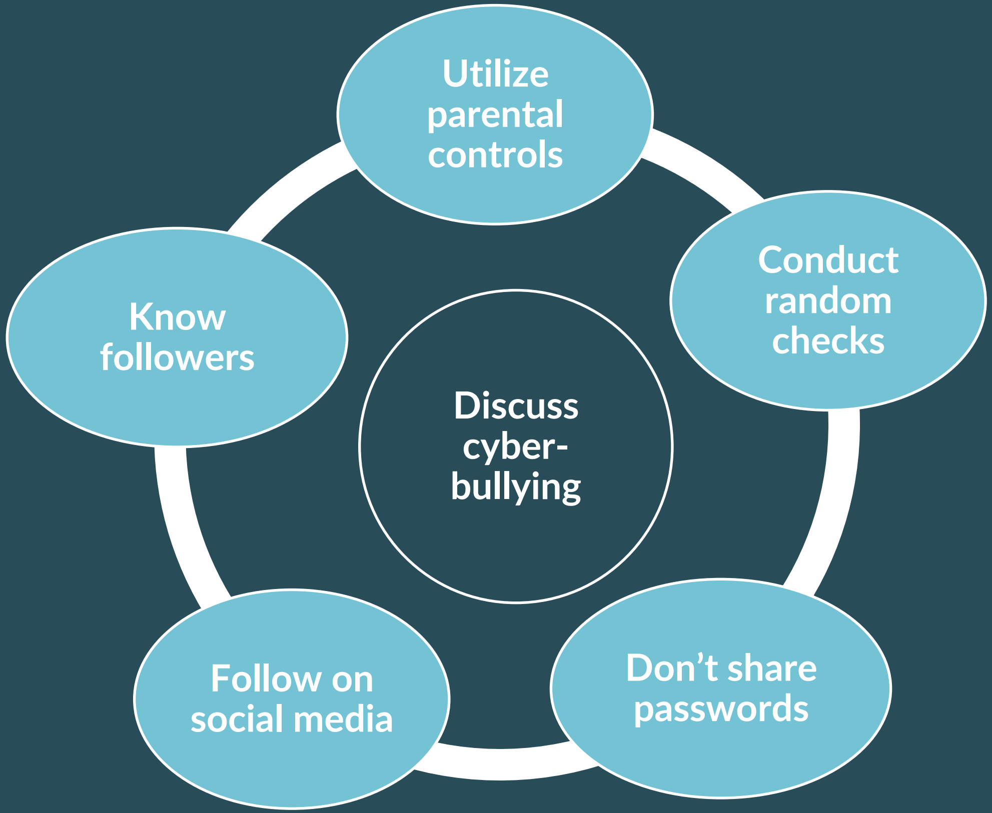
Beware of phishing emails

Use strong passwords

1-05235763

Protecting Your Family

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



Discuss cyber-bullying

Utilize parental controls

Conduct random checks

Don’t share passwords

Follow on social media

Know followers

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

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

jfgfasupport@johnsonfinancialgroup.com

JohnsonFinancialGroup.com