AVOIDING COVID-19 SCAMS

MONDAY, MAY 4 @ 6:30-7:30PM
SSSI and Veterans Affairs Benefit Recipients with Dependents: Register by May 5

St. Louis County Small Business Relief Program
Up to $15,000 grant
http://stlcorona.com/resources/small-business-relief-program/
Red Backpack fund
$5,000 grant
May Deadline: 5/11/20 at 11 a.m. CST
https://www.globalgiving.org/red-backpack-fund-faq/
UMSL College of Business Midwest Digital Marketing Conference
May 20-21 Virtual Conference
May 25-29 On Demand Sessions
https://bestmarketingconference.com/index.php
MISSION

Legal Services of Eastern Missouri advances justice through legal representation, education and supportive services. We partner with the community to improve lives, promote fairness and create opportunities for those in need.
WHO WE ARE

The Coalition is a diverse group of community stakeholders who are dedicated to increasing family self-sufficiency and prosperity through financial education and asset-building.

MISSION

Promoting equitable opportunities for financial health to build wealth and economic prosperity.
Public awareness campaign designed to help consumers better manage their personal finances. This is achieved through the collaboration and coordinated effort of hundreds of organizations across the metro area, including businesses, financial institutions, schools, libraries, not-for-profits, etc.
COVID-19 SCAMS and Avoiding Them

- Coronavirus Stimulus Payment Scams
- Links in Unsolicited Text Messages
- Beware of MLM Companies
- Section 8 Scammers
- Telework Vulnerabilities
- Education Technology Services and Platforms
- Business Email Compromise (BEC)
- General Cyber Crime Vulnerability Tips
Coronavirus Stimulus Check Scams

Scammers are using CARES Act relief payments as the basis for a variety of scams.

**TRICK:** “Pay a fee to get your payment right away.”

*No one must pay a fee to get a relief payment.*

Report scams to the Federal Trade Commission: [www.ftc.gov/complaint](http://www.ftc.gov/complaint)
Coronavirus Relief Check Scams

TRICK: “We need your Social Security / Bank Account / Benefits Card number to confirm your payment.”

You will never be called by the IRS to get this kind of information.

Report scams to the Federal Trade Commission: www.ftc.gov/complaint
Coronavirus Relief Check Scams

TRICK:
“We actually overpaid you. Please send a check back to us right away for the overpayment.”

*You should never* trust a call or email for a check to be returned.

Report scams to the Federal Trade Commission: www.ftc.gov/complaint
4 Tips For Avoiding A Coronavirus Stimulus Payment Scam

1. Anyone who asks you for personal information is phishing! Learn more at www.consumerftc.gov/articles/how-recognize-and-avoid-phishing-scams

2. ONLY USE the IRS website:


   to submit information to the IRS – never in response to a call, text, or email.
You **NEVER** have to pay to get your relief payment.

The IRS won’t tell you to deposit your check, then send some or all of it back. That’s a fake check scam.

Unsolicited Text / Email Messages

Avoiding a Coronavirus Text / Email Message Scam

You might be seeing text messages promising:

- Tests for COVID-19
- Loans for small businesses, or
- Money for quarantined people

www.ftc.gov/coronavirus/scams-consumer-advice
Unsolicited Text / Email Messages

Avoiding a Coronavirus Text Message Scam

Scam artists use government logos, important sounding language, and other tricks to get you to believe the message is legitimate.

NO government agency will send messages like this! If you ever doubt a message is real, don’t respond to it.

Instead, look up the agency or person and contact them on your own.

www.ftc.gov/coronavirus/scams-consumer-advice
PRO TIP: The more errors a text or email has, the more likely it is a scam. Why?

Scammers know that those who don’t notice the mistakes, are more likely to fall for the scam.

Better to filter out people who spot errors and ask too many questions!
Unsolicited Text Messages

Tips to Avoid a Coronavirus Text Message Scam

1. Do not click on any links. Clicking could expose you to scams, download malware, or get your phone number added to lists that are then sold to other bad actors.

2. Delete those text messages immediately.

The Federal Trade Commission announced on April 24, 2020 that it has sent 10 letters warning multi-level marketing companies (MLMs) to remove and address claims that they or their participants are making about their products’ ability to treat or prevent coronavirus disease or about the earnings people who have recently lost income can make, or both.

“MLMs and other companies that distribute their products through networks of distributors are responsible for the product and earnings claims those distributors are making. During this health and economic crisis, we are on the lookout for false income claims for work-at-home opportunities, in addition to spurious health claims that products can treat or prevent COVID-19.”

Andrew Smith
Director of the FTC’s Bureau of Consumer Protection.
FTC Warns Multi-Level Marketing Companies

MLMs’ distributors posted their unsupported ads on social media sites.

“Need to make extra money? Find it difficult to pay your bills? Were you laid off/ fired? Be your own Boss w/doTERRA essential oils. Msg me to achieve financial independence #laidoff #unemployed #cantpaymybills #cantpaymyrent #student #sales #sidehustle #makemoney #stayathomemom.”

“...Living in quarantine and where 14 million people applied for unemployment just last week ... I’ll stick with the opportunity to change people’s lives ... turn a small investment into six figures .... #arbonne ... #quarantine #2020”

“[E]veryone’s getting stimulus checks right now... There is no better investment you could do... Take that money that you’re about to get back... figure out a way to make this happen tonight.”
FTC Warns Multi-Level Marketing Companies

Before Joining a Multi-level Marketing Company…

Most people who join legitimate MLMs make little or no money.

If you’re thinking about joining an MLM company, get the details. Start by searching online for the name of the company and words like review, scam, or complaint.

Be skeptical of portrayals of lavish lifestyles made possible by participating in the program.

If promoters emphasize recruiting as the real way to make money, head for the exit.
Section 8 Scammers

Official Housing Authority Websites
Section 8 Scammers

Tips to Avoid Section 8 Scams

1. Contact your local housing authority to find out how to register for the Section 8 waiting list lottery. You’ll find their email and phone number on the HUD site. Follow their instructions to sign up.

2. Housing authorities do not charge fees, and they won’t reach out to you by phone or email to suggest that you join a waiting list. A housing authority also will never ask you to wire money or pay with a prepaid card. Those are sure signs of a scam. (https://www.consumer.gov/articles/1019-money-wiring-scams)

3. Protect your Social Security number and other personal information (say, credit card numbers). Don’t give them out on a website you find through a random search.
KEEP CALM and Avoid Coronavirus Scams

Here are 5 things you can do to avoid a Coronavirus scam:

Federal Trade Commission

If you see a scam, report it to ftc.gov/complaint
1. Ignore offers for vaccinations and home test kits.
   Scammers are selling products to treat or prevent COVID-19 without proof that they work.

2. Hang up on robocalls.
   Scammers use illegal sales call to get your money and your personal information.

3. Watch out for phishing emails and text messages.
   Don’t click on links in emails or texts you didn’t expect.
Research before you donate.
Don’t let anyone rush you into making a donation. Get tips on donating wisely at ftc.gov/charity.

Stay in the know.
Go to ftc.gov/coronavirus for the latest information on scams. Sign up to get FTC’s alerts at ftc.gov/subscribe.

Federal Trade Commission
If you see a scam, report it to ftc.gov/complaint
Software from Untrusted Sources

Ex. Malicious cyber actors may use legitimate-looking telework software—which may be offered for free or at a reduced price—to gain access to sensitive data or eavesdrop on conversations.

Ex. Cyber actors may also use phishing links or malicious mobile applications that appear to come from legitimate telework software vendors.
Software from Untrusted Sources - TIPS

- Select trusted and reputable telework software vendors; conduct additional due diligence when selecting foreign-sourced vendors.
- Beware of advertisements or emails purporting to be from telework software vendors.
- Avoid phishing! Make use of tools that block suspected phishing emails or allow users to report and quarantine them.
- Verify the web address of legitimate websites or manually type it into the browser.
- NEVER open attachments or click links within emails from senders you do not know – or attachments you don’t expect.
Working from Home Vulnerabilities

Use Communication Tools Wisely: (Zoom, Teams, Slack, Skype, Google Meet, Etc.)

Tips

• Restrict access to remote meetings, conference calls, or virtual classrooms.

• Use passwords if possible (and don’t share the password and login together).

• Do Not Share web links on the public web! Hackers can “crawl” the entire world wide web to find links to meetings. (“ZOOM bombing”).

• Send meeting invites with encrypted messaging apps or email.
Business Email Compromise

BEC is a scam that targets both individuals and businesses who have the ability to send wire transfers, checks, and automated clearing house (ACH) transfers.

Ex. the victim receives an email purported to be from a company the victim normally conducts business with; however, the email requests money be sent to a new account, or for standard payment practices be altered.
Business Email Compromise

Look out for:

- The use of urgency and last-minute changes in wire instructions or recipient account information;
- Last-minute changes in established communication platforms or email account addresses;
- Communications only in email and refusal to communicate via telephone;
- Requests for advanced payment of services when not previously required; and
- Requests from employees to change direct deposit information.
Do:

- Check for last-minute changes in wiring instructions or recipient account information.
- Verify vendor information via the recipient's contact information on file—do not contact the vendor through the number provided in the email.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.
- If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds, and contact your employer to report irregularities with payroll deposits. As soon as possible, file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov or, for BEC and/or email account compromise (EAC) victims, BEC.IC3.gov.
Today's rapid incorporation of education technology ("edtech") and online learning could have privacy and safety implications if students' online activity is not closely monitored. Parents and caretakers should be aware of new technology issued to children who do not already have a foundation for online safety.
Example Hack:
Cyber actors exploited school information technology (IT) systems by hacking into multiple school district servers across the United States.

- Accessed student contact information, education plans, homework assignments, medical records, and counselor reports
- Used that information to contact, extort, and threaten students with physical violence and release of their personal information.
- Also sent text messages to parents and local law enforcement, publicized students' private information, posted student personally identifiable information on social media, and stated how the release of such information could help child predators identify new targets.
School at Home: Tips

**Do:**
- Closely monitor children's use of edtech and online services.
- Find out who can see, use, or sell data. Who will tell if there’s a data breach? Can child’s data be deleted? Completely?
- “Google” your child. See what you find on the web about them from their use of edtech.
School at Home: Tips

Don't:

• Provide exact information on children when creating user profiles
  o use initials instead of full names,
  o avoid using exact dates of birth,
  o avoid including photos
• Never assume the school “knows better” than you. If you have concerns, ask the school!
General Cyber Crime Vulnerability Tips

Tips to protect individuals and businesses from cybercrimes / hackers:

**Do:**
- Change passwords for routers and smart devices from default setting to unique passwords.
- Check for misspelled domain names within a link
- Use multi-factor authentication (MFA) when accessing organizational sites, resources, and files.
- Practice good cyber security when accessing Wi-Fi networks, including use of strong passwords and Wi-Fi Protected Access (WPA) or WPA2 protocols.
- Ensure desktops, laptops, and mobile devices have anti-virus software installed and routine security updates are applied; this includes regularly updating web browsers, browser plugins, and document readers.
General Cyber Crime Vulnerability Tips

Tips to protect individuals and businesses from cybercrimes / hackers:

Don’t:

• Open attachments or click links within emails received from senders you do not recognize.
• Provide usernames, passwords, birth dates, social security numbers, financial data, or other personal information in response to an email or phone call.
• Use public or non-secure Wi-Fi access points to access sensitive information.
• Use the same password for multiple accounts.
Additional COVID-19 updates available online: 
https://lsem.org/covid-19-updates/
Questions? Comments?

Downloads for this presentation:

https://t2m.io/dk0XuC3g

Password: MoneyMondays