COVID-19 SCAM INFORMATION and GUIDANCE

Types of Scams

Government Impersonators

One of the most prevalent schemes we're seeing is government impersonators. Criminals are reaching out to people through social media, emails, or phone calls pretending to be from the government. In some cases, they're even going door-to-door to try to convince someone that they need to provide money for COVID testing, financial relief, or medical equipment.

We are a very trusting society, but it's important to know that the government will not reach out to you this way. If someone reaches out to you directly and says they're from the government helping you with virus-related issues, it's likely a scam. This "government" representative may be trying to use phishing or other techniques to hack your computer or get your personal information or money.

Fraudulent Cures or Medical Equipment

Right now, the threat we're most concerned about is fake cures or treatments for the virus. These "cures" can be extremely dangerous to your health-even fatal. You should never accept a medical treatment or virus test from anyone other than your doctor, pharmacist, or local health department.

Work-from-Home Fraud

People who are at home and out of work are vulnerable to work-from-home scams. If someone you don't know contacts you and wants you to urgently pay them in return for a "job," you are

dealing with a criminal. Legitimate jobs will not ask you to pay them.
If you're in a role like this where you're being asked to send or move money, you're acting as a Money Mule which is a federal crime.

Investment Fraud

One of the most lucrative schemes for criminals is offering you an opportunity to invest in a cure or treatment for the virus. The purpose of these get-rich-quick schemes is simply to defraud the investor. Any offer like this should be treated with extreme caution.

Tips for Prevention

- Avoid clicking on links in unsolicited emails and be wary of email attachments, even from sources that appear to be legitimate. Malicious actors have been sending phishing e-mails designed to appear as if they are coming from the U.S. Centers for Disease Control ("CDC"), healthcare specialists and employers, all with seemingly "urgent" safety messages and health information.
- Always "mouse" or "hover" over the e-mail senders name to determine the true origin.
- Never reveal personal or financial information via e-mail. Remember, EOTSS will never ask you for your username or password.
- Do your homework before making any donations. Be wary of someone asking for "urgent" donations in cash or gift cards. Always verify a charity before making donations. You can visit the **Federal Trade Commission's** site for more information.

- Up to date scam information from the Department of Homeland Security **National Cyber Awarness System** and the **Department of Justice**.
- Remember, there is not currently a vaccine available for COVID-19. Any solicitation suggesting they've discovered a cure should be deleted and/or ignored.
- For the most up-to-date information about the Coronavirus, visit trusted sources such as the **Massachusetts Department of Public Health**, **Centers for Disease Control and Prevention** (CDC) and the **World Health Organization** (WHO).