COVID-19 and the Proliferation of Fraud

As the COVID-19 pandemic continues to negatively impact human health and economic stability, fraud has emerged as another significant problem in light of the crisis. Unfortunately, in the wake of the pandemic, many fraudsters and scammers have seized the opportunity to take advantage of vulnerable Americans.

According to the Association of Certified Fraud Examiners, most fraudsters are under financial distress when they commit acts of fraud, a situation many Americans currently face. As of May, despite the Department of Labor's estimated 13.3% unemployment rate, the Brookings Institution posits that it actually sits closer to 19% due to worker classifications within the Payroll Protection Program. Either way, these are the highest levels of unemployment recorded since the Great Depression. Clearly, economic distress is off the charts, compared to normal times.

With this in mind, one must approach all online activity with care. Here are seven scams you should beware:

1. The Justice Department warns of an increase in the impersonation of government and healthcare officials, particularly via "phishing". Phishing involves an email aimed at luring an individual to provide sensitive data such as banking details or personal identification information.
2. Loan and procurement fraud are on the rise as trillions of dollars are have been injected into the economy. Beware of the red flags of fraudulent activity such as bribes and kickbacks, including the involvement of an unnecessary broker or middleman in transactions, or unjustified favoritism of a particular contractor.
3. Business email systems are also being targeted by scammers looking to make fraudulent money transfers or to spread malware, accomplished through the impersonation of a company employee. The finance industry is especially susceptible, and these problems can cost companies significantly.
4. Some hackers have targeted Zoom, a critical component of the online workplace. Forbes reported in April that cyber risk assessment experts at Cyble discovered that hackers had stolen half a million personal Zoom credentials (including passwords!) and sold them for a small profit.
5. Cryptocurrency fraud is on the rise, occurring thanks to fake websites and mobile applications designed to closely resemble those of valid companies, like Bitcoin. These sites are often missing the "https" in the web address, while apps have warning signs including spelling mistakes and modified logos.
6. Charity fraud has become more common as many fraudsters create convincing yet false donation pages to collect funds intended to support other COVID-19 related funds and causes.
7. A final risk is online predatory behavior targeted at children. Many children are online more frequently for school and leisure, but they are also more anxious and isolated; dangerous predators can take advantage of these conditions, and UNICEF warns of an increase in grooming, sexting, and trafficking.

These are just a few of the most common fraudulent behaviors that have increased during the pandemic. So, what can you do? There are many practices that you can adopt to help your business and family enjoy safer online activity or, if necessary, respond to fraud.

1. Verify the legitimacy of financial and charitable institutions, as well as the institution's website.
2. Be extremely selective when filtering unsolicited calls and emails, especially being careful not to share sensitive personal information.
3. Watch out for unusual payment requests or changes to normal business requests, and double check legitimacy. These emails could include an emergency payment request from an executive, or an email listing a new account number for a payment to a supplier.
4. Do research before making any sort of online payments.
5. Follow the Small Business Administration's safe processes when applying for government loans.
6. Check with vendors and partners to see how they are handling fraud.
7. Require a 'second set of eyes' for approval of large transactions within your day-to-day operations.
8. Familiarize your employees with fraud risks and safe practices.
9. If dealing with fraud involving foreign entities, The Foreign Corrupt Practices Act of 1977 applies to foreign firms and persons that cause furtherance of corrupt payment within the U.S. You can seek the advice of legal counsel or submit FPCA violations Fraud Section of the Department of Justice.

If you experience fraud during the pandemic, you can report it to the National Center for Disaster Fraud Hotline, at 866-720-5721, or visit their website to submit a web complaint form.

Many of these practices seem obvious, but in a period of high stress and rapid change in online ecosystems, we all are more susceptible than we may realize.