Cyber Prep 101: You Don't Have To Be A Victim

Dr. Shawn P. Murray, C|CISO, CISSP, CRISC

Colorado SBDC TECHSOURCE
CYBER: Cover Your Assets™

NCC National Cybersecurity Center

www.pikespeaksbdc.org

El Paso County Economic Development · Ent Business Banking · Colorado Springs · PSBTrust.com Park State Bank & Trust · CenturyLink · Colorado Springs Utilities It's how we're all connected · VectraBank Colorado · Powered by SBA U.S. Small Business Administration

Funded in part through a cooperative agreement with the U.S. Small Business Administration

The Pikes Peak SBDC's Cyber: CYA program is built to assist small and medium sized businesses by focusing on topics for all levels of business and their needs from cloud computing, security measures using social media, to securing technology to meet compliance standards in government contracting.

Free and confidential consulting and low-cost workshops are available! Browse our resources and workshops at www.pikespeaksbdc.org/cyber

Free Consulting | Practical Training | Cyber Resources

Micki Cockrille

Marketing Manager
National Cybersecurity Center

Micki Cockrille is the Marketing Manager for the National Cybersecurity Center in the Pikes Peak Region where he has lived for 24 years. A 2019 Colorado Springs Business Journal Rising Star, Micki has collaborated with several Southern Colorado nonprofit and startup organizations. Micki now sits on the board of directors for local nonprofit REACH Pikes Peak. In his spare time, Micki loves chasing passions in music, Colorado outdoors, food, gaming, and friends and family.

Dr. Shawn Murray

SBDC TechSource: Lead Cyber Consultant & Covid-19 Team Member

Shawn Murray is a Principal Scientist and the President/CEO at Murray Security Services. He is assigned to the U.S. Missile Defense Agency as a Senior Cyber Security Professional and is an officer in the U.S. Civil Air Patrol. Dr. Murray has worked with the NSA, FBI, CIA and the U.S. Defense and State Departments on various cyber initiatives and has over 20 years of IT, Communications, and Cyber Security experience. His previous assignments include work with the U.S. Army Cyber Command in Europe, the U.S. Air Force, and with commercial industry in various roles of Information Assurance and Cyber Security. He has traveled the globe performing physical and cybersecurity assessments on critical national defense and coalition programs and has prepared reports for the House Armed Services Committee. Dr Murray also serves on the International Board of Directors for the Information Systems Security Association.

View Consultant Bio or Schedule Consulting

Colorado SBDC TECHSOURCE
CYBER: Cover Your Assets

Workshop Overview/Today's Agenda

Topics include…

- Scams
- Privacy
- Remote working during a pandemic
- Analyze what you are doing
- Business Continuity
- Questions

Scams!

- Many businesses have been introduced to scams over the past several months and some are very effective!
  - COVID PPE Scams
  - Loan Scams
  - Misinformation scams

1. **PUBLIC HEALTH SCAMS**
2. **GOVERNMENT CHECK SCAMS**
3. **BUSINESS EMAIL SCAMS**
4. **I.T. SCAMS**
5. **SUPPLY SCAMS**
6. **ROBOCALL SCAMS**
7. **DATA SCAMS**

https://www.ftc.gov/news-events/blogs/business-blog/2020/03/seven-coronavirus-scams-targeting-your-business

Re: COVID-19 Adjustment ! Spam ×

Admin Department
to me

1:20 PM (3 hours ago)

This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe

Dear Staff

New notification ,Please due to COVID-19, all staff & Employee are expected to kindly Click PROCEED and complete the required directive to be added to March and April benefit payroll directory as compilation is ongoing and will last within 48hours.

Thank you,
Admin Department

Federal Bureau of Investigation
Internet Crime Complaint Center(IC3)

Contact the FBI's IC3 to file a complaint:

https://www.ic3.gov/default.aspx

SERVICES

Report Fraud Waste and Abuse

COVID-19 Scams

Report Scam Attempts

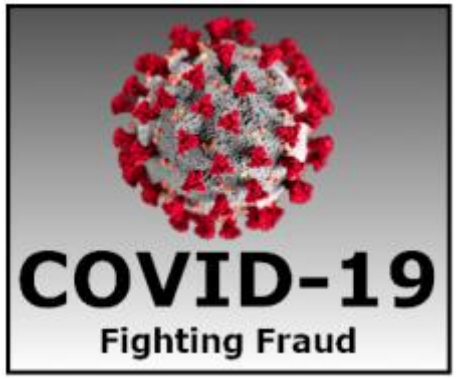
Report Fraud or Misconduct Related to Government Contracts or Grants

COVID-19 Scams

If you receive calls, emails, or other communications claiming to be from the Treasury Department and offering COVID-19 related grants or stimulus payments in exchange for personal financial information, or an advance fee, or charge of any kind, including the purchase of gift cards, please do not respond. These are scams. Please contact the FBI at www.ic3.gov so that the scammers can be tracked and stopped.

Fraud involving payment of **Federal taxes** should be reported to the Treasury Inspector General for Tax Administration.

https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams



COVID-19 Consumer Warnings and Safety Tips

As the novel coronavirus (COVID-19) pandemic continues to impact the United States, phone scammers have seized the opportunity to prey on consumers.

The FCC has received reports of scam and hoax text message campaigns and scam robocalls offering free home testing kits, promoting bogus cures, selling health insurance, and preying on virus-related fears.

A text message scam may falsely advertise a cure or an offer to be tested for coronavirus. Do not click on links in texts related to the virus, and check cdc.gov/coronavirus for the most current information.

Some text scams are impersonating government agencies. The FCC recently learned of a text scam claiming to be from the "FCC Financial Care Center" and offering $30,000 in COVID-19 relief. There is no FCC program to provide relief funds to consumers. The text is likely a phishing attempt to get banking or other personal information from victims. The BBB is also warning of a text message scam impersonating the U.S. Department of Health and Human Services informs recipients that they must take a "mandatory online COVID-19 test" using the included link.

https://www.fcc.gov/covid-scams

COVID-19 Consumer Warnings and Safety Tips

Sample Hoax Text

From my next door neighbor

Just received this...from good friend of mine who works for the CDC

Please be advised, within 48 to 72 hours the president will evoke what is called the Stafford Act. Just got off the phone with some of my military friends up in DC who just got out of a two hour briefing. The president will order a two week mandatory quarantine for the nation. Stock up o whatever you guys need to make sure you have a two week supply of everything. Please forward to your network.

Coronavirus Scam Audio Samples

Test Kit Phone Scam

▶ 0:06 / 0:15

Audio transcript: *...[The Coronavirus] Response Act has made coronavirus testing more accessible immediately. If you want to receive a free testing kit delivered overnight to your home, press 1. If you do not want your free testing, press 2.* (Audio source: YouMail)

Student Loan Callback Scam

▶ 0:03 / 0:36

Audio transcript: *Hello this is Brad ... with an important message regarding the effects of the coronavirus outbreak on your student loans. As you may have already heard, President Trump invoked his power as commander-in-chief by declaring a national emergency due to the widespread impact of COVID-19. New measures will include waiving interest on your federal student loans until further notice. During this time our offices have continued to maintain full staffing levels and will continue to do so until further notice. For more information on how these new measures will impact your future payment obligations, call us back today at 855-264-XXXX before 6:00 PM Pacific Standard Time. Thanks, and have a great day* (Audio source: Nomorobo)

https://www.fcc.gov/covid-scams

Did you know that Colorado has one of the most stringent cyber security and privacy laws in the United States?

- It applies to all businesses (in or out of Colorado) that target Colorado citizens as clients or customers.
- It does not matter the size of your business!
- If you process, transmit or store privacy information on a CO citizen, the law applies and you have to protect their information.
- The law redefines PII as any public information combined with a unique identifier like:
  - Your Social Security Number,
  - Your EDPI number,
  - Your Student ID number or
  - Your driver's license number.

Why should you care?

- Many businesses are using collaboration platforms to conduct business remotely. Some platforms include links to other things outside of their platform that may not be known.
- Examples include:
  - MS Teams
  - Zoom
  - GoToMeeting
  - WebEx
  - Facebook Live
  - Skype
  - Other less know platforms

Why should you care?

- The key take away if you use remote computing technology:
  - **SECURE THE TECH!**
    - All technology has settings for security and registration, be sure to configure it!
  - Understand where the tech is communicating to.
  - Understand what the tech is doing with yours and your customer's data.
  - This should include analytics software to track what users are doing.

Hackers are selling two serious Zoom zero-day vulnerabilities for $500,000

By Mark Wyciślik-Wilson | Published 23 hours ago

Both the Windows and macOS versions of Zoom have critical, unpatched security vulnerabilities that could be exploited by hackers to target users and spy on calls and meetings.
Security experts say -- despite not having seen the actual code for the exploits -- that the Windows version of Zoom is affected by an RCE (Remote Code Execution) described as being "perfect for industrial espionage". The zero-days have been offered for sale for $500,000.

See also:

1. Hundreds of thousands of stolen Zoom accounts for sale on hacker forums for next to nothing
2. Zoom will soon let some users choose which countries their data is routed through
3. Zoom is taking steps to improve privacy and security, and to prevent Zoombombing

As reported by Vice's Motherboard, three separate sources have confirmed that the vulnerabilities are available to buy in hacking circles, and have been offered to these individual directly. News of the zero-days comes just days after it was reported that hacker forums are being used to offer Zoom user credentials for sale at incredibly low prices.

Zoom apologises for major security vulnerabilities, promises fixes

By Mike Moore 14 days ago

Questions raised around Zoom security and safety

Many businesses are allowing employees to use personal computers to perform work remotely.

- While this may provide convenience for the employer, it also introduces risk!
  - How is your business information protected?
  - What is the sensitivity of the data?
  - How is the information, files, folders data backed up?
  - What is the security posture of the employees' computers or home networks?

Many businesses have moved to remote storage for saving and sharing files.

- Examples include:
  - Dropbox
  - Google Drive
  - MS One Drive
  - Apple storage (for computers and mobile devices)
  - Other solutions as well.
- The key take away if you use remote computing technology:
  - **SECURE THE TECH! (Yes, this is a repeat!)**
    - All technology has settings for security and registration, be sure to configure it!
  - Consider the sensitivity of your information or data.

Business Continuity Considerations

- While many have adapted to the “New Norm” of working remotely, the initial focus was on getting everyone set up to do so. One of the questions you should ask now is how resilient is your business?
  - Ask your self these questions and develop a plan to address areas where you think you may have risk:
    - What information or data does my business produce that is considered critical?
    - Where is it processed, transmitted or stored?
    - How is it protected? (IE: encrypted, backed up etc.)
    - Who has access to it? (internally and externally)
    - **TRAIN, TRAIN, TRAIN! (employees, vendors, consultants etc.)**

What can you do as a small business?

- Categorize and classify your information/data
  - Develop an information and data classification scheme
- Categorize and classify your systems
  - Align the scheme above to the systems you use to process transmit & store sensitive data
- Perform an inventory
  - See what laws apply to your business processes
- Develop a plan
  - Determine what applies to your organization
- Talk to an SBDC Consultant
  - Make an appointment to get assistance!

Questions?

www.pikespeaksbdc.org

El Paso County Economic Development · Ent Business Banking · Colorado Springs · PSBTrust.com Park State Bank & Trust · CenturyLink · Colorado Springs Utilities · VectraBank Colorado · Powered by SBA

Funded in part through a cooperative agreement with the U.S. Small Business Administration