Business System Solutions

Caretakers of Your Productivity
since 1995

THE BSS ADVISOR

Monthly Newsletter

October 2024

Reporting Cybercrime & Resources to Save You

Photo by Pixabay/Vlansuan from Pexels

The first step toward bringing cybercriminals to justice is reporting cybercrime when it happens.

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. We are the Caretakers of Your Productivity.

With Offices in:
North Central Indiana
(765) 742-3440

Middle Tennessee
(615) 819-0600

West Michigan
(616) 776-0400

info@bssconsulting.com

"Do not be anxious about anything, but in every situation, by prayer or petition, with thanksgiving, present your requests to God."
Philippians 4:6

Cybercrime can be difficult to investigate and prosecute because it often crosses legal jurisdictions, even international boundaries. Offenders often disband online criminal operations and launch new ones at a rapid clip. This constant churn means authorities often work one step behind the hackers.

Authorities have seriously upped their game since the first viruses, malware, and phishing attacks hit. Federal, state, and local law enforcement are hyper-focused today on becoming ever more sophisticated about cybercrime. Billions of dollars in resources are devoted to preventing, stopping, and investigating cyber threats. Legislation continues to be passed that further empowers federal, state, and local authorities to bring cybercriminals to justice and show the world that crime doesn't pay, even on the internet.

But at the end of the day, stopping cybercriminals begins with you. If you are a target of cybercrime, it cannot be rectified unless the authorities are aware of it. This is also true if you were just a potential target of an attack, such as a phishing email or text links. Depending on the nature of the attack, reporting a cybercrime can be as simple as clicking a button in your email program.

Remember, you aren't alone online: You have the power to stop cybercriminals and there are many resources available to assist you.

(Continued on Next Page)

(Continued from page 1)

Step 1: Get Help Immediately


Photo by Pixabay/Rikk32

Your workplace's IT department: If the cybercrime happened at work, you should contact a supervisor or your company's IT department. It is very important that you report the situation immediately – cybercriminals might be targeting your company so early detection can be critical in stopping this.

Local Law Enforcement: Even if you are the target of a multinational cybercrime, your local law enforcement agency (such as your local police department or sheriff's office) has an obligation to assist you by taking a formal report. They are also required to make referrals to other agencies, when appropriate. Report your situation as soon as you find out about it. Nowadays, many local and state agencies have detectives or departments that focus specifically on cybercrime.

Your email provider – Report as Phishing or Spam: Deleting spam, malicious messages or any other suspicious emails keeps you safe, but you can bolster your cybersecurity by reporting any serious cybercrime attempt to your IT department or email client. Many of the major email services (like Gmail and Outlook) make this very easy to do. You can also block senders, so you can ensure a bad actor email account never contacts you again, but bear in mind, the bad guys change email addresses and spoof legit ones faster than a game of Whack-a-Mole.

The Internet Crime Complaint Center (IC3): IC3 is a partnership between the Federal Bureau of Investigation (yes, that FBI) and the National White Collar Crime Center (funded, in part, by the Department of Justice's Bureau of Justice Assistance). IC3 will thoroughly review and evaluate your complaint and refer it to the appropriate federal, state, local or international law enforcement or regulatory agency that has jurisdiction over the matter. File your complaint with the IC3 at https://ic3.gov.

Federal Trade Commission (FTC): While the FTC does not resolve individual consumer complaints, it does run the Consumer Sentinel, a secure online database used by civil and criminal law enforcement authorities worldwide to detect patterns of wrong-doing. Nailing down patterns leads to investigations and prosecutions. You can file your complaint to the FTC at https://reportfraud.ftc.gov. Find more resources aimed at individuals, businesses and law enforcement at https://identitytheft.gov.

Local victim services provider: Because cybercrime has impacted so many people across the country, many communities in the United States actually have victim advocate initiatives to help you. These advocates can help you with resources, emotional support and advocacy. Find local victims service providers at https://ovc.ojp.gov/directory-crime-victim-services/search.

Step 2: Collect and Keep Evidence

Disconnect from the internet but don't turn off that computer or phone. There is specific information saved in memory that your IT or law enforcement can use; it may disappear if you restart your device.

(Continued from page 2)

Dust off your detective hat. You might not be asked to provide evidence when you initially report cybercrime, but it is imperative that you keep any evidence related to the complaint. That phishing email, suspicious text or ransomware isn't just bits and bytes – it's evidence. This material can help law enforcement stop and prosecute hackers.

Keep items in a safe location in the event you are requested to provide them for investigative or prosecutive evidence. All of the following documentation might be considered evidence, but you should keep anything you think could be related to the incident, such as:

Certified or other mail receipts; Chatroom or forum conversations; texts/SMS messages; Credit card receipts; Envelopes & shipping materials; Computer Log files; Social media messages; Money order & wire receipts, or canceled checks; Pamphlets or brochures; Phone bills; Copies of emails, preferably electronic copies. If you print the email, include full email header information; and Copies of web pages, preferably electronic.

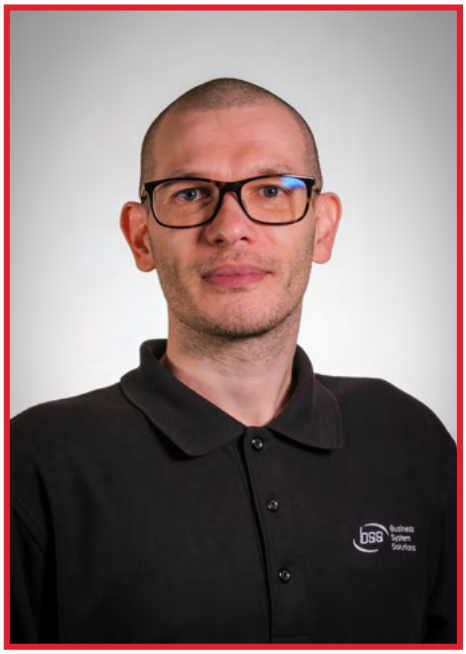
Provide everything you can, including a timeline, to your IT department and local law enforcement. It can all help to identify and stop the threat, help you recover more quickly, and prevent others from becoming a victim.

Additional Resources

There are many companies, government, and law enforcement agencies that have expertise and copious financial resources to help you survive and overcome a cyberattack. You don't have to go it alone! See the full article and links to all the additional resources available to you at the National Cybersecurity Alliance: https://staysafeonline.org/resources/reporting-cybercrime/

The National Cybersecurity Alliance is a non-profit organization on a mission to create a more secure, interconnected world. They advocate for the safe use of all technology and educate everyone on how best to protect ourselves, our families, and our organizations from cybercrime. They create strong partnerships between governments and corporations to amplify our message and to foster a greater "digital" good. They offer resources and education for individuals, companies of all sizes, and parents to help keep their kids safe online. □

Employee Highlight: Ivan Boranov



Ivan Boranov is a newer addition to our Grand Rapids, Michigan office, as a Security & Compliance Administrator. He has been working in IT since 2018 and brings a wealth of knowledge and certifications to us.

His education includes a Masters in Cybersecurity and a bachelors in Business Administration, among many high level IT certifications such as Microsoft Azure Fundamentals, CompTia Security+, and Oracle Cloud Data Management and Infrastructure.

Before his deep dive into IT, Ivan was a chef and pastry chef with yet another degree in Culinary Arts. A connoisseur of cooking, we're placing our bets on a winning recipe for the upcoming BSS Chili Cookoff.

In his spare time, he volunteers for local animal shelters and dreams of creating animal rescue sanctuaries for his furry friends to live out their lives in comfort and play. We are so grateful to have his calm expertise helping our clients!

Business System Solutions

Return Address:
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544

The BSS ADVISOR

info@bssconsulting.com

North-Central Indiana Office
1211 Cumberland Avenue
West Lafayette, IN 47906
(765) 742-3440

Middle Tennessee Office
1026 West College Street
Murfreesboro, TN 37129
(615) 819-0600

West Michigan Office
601 3-Mile Road NW, Suite C
Grand Rapids, MI 49544
(616) 776-0400

6 Years in a Row!
2019-2024 Winner
Channel Futures.
Leading Channel Partners Forward
MSP 501

Time for Indiana Fall Cleanup!

2024

ELECTRONIC WASTE RECYCLING DRIVE

Business System Solutions

1211 Cumberland Avenue
West Lafayette, IN

Visit us online at
www.bssconsulting.com/ewaste
for more information

We CANNOT accept: ANY lightbulbs, Refrigerators, Stoves, Washers, Dryers, Wood, Paint, Chemicals, etc.,

Accepting ALL electronics *FREE of charge

*$20 Fee to recycle old CRT monitors and box TVs
CASH ONLY

OCTOBER 16 & 17
8:00 AM - 5:00 PM