CTSI
TECHNICAL UPDATE
Volume 27 Number 40 | October 3, 2023

CYBERSECURITY REMINDERS: REMOVABLE MEDIA AND INVOICE FRAUD

Removable media, such as USB drives, external hard drives, SD cards, CDs, and even smartphones, can pose several risks if not managed properly. To minimize these risks it is important to educate employees about the potential hazards and establish policies for its proper use.

More often than they would like, businesses record a significant loss of money due to invoice fraud. In the last 3 years, a 75% increase in payment request fraud has been detected, leaving businesses of all sizes with substantial financial losses.

WHY IS REMOVABLE MEDIA A RISK?

DATA OUT

In a hybrid work environment, we may copy files to a drive to take home with us. These drives (or any removable media) are much easier to lose than a laptop or tablet. If sensitive data, private information, or files proprietary to the company are held on the drive, it can be disastrous if lost. In one study researchers dropped nearly 300 USB sticks on a university campus. 98% of the drives were picked up and 45% of those picked up, the individual finding it clicked on the files inside to open them. Losing such a drive can result in sensitive data being viewed, used, or sold by unauthorized parties or a loss of trust in an organization with a formerly good reputation.

DATA IN

Malware attacks originating on USB drives are increasingly common. When a USB drive with the malware is plugged into a computer it launches a program that creates a backdoor and exfiltrates files of interest, keystrokes being made on the keyboard of the computer, and screenshots of the activity of the now compromised computer. Other similar malware programs have granted backdoor remote control access to infected computers.

Kindly refuse if a client or vendor asks you to plug in a drive to your computer. We recommend only plugging in drives from trusted sources. If necessary, you may consider disconnecting from the Internet, changing from Wi-Fi to airplane mode, and then plug in the drive. Right-click on the drive in File Explorer and choose "Scan with … antivirus". After it has finished the scan, if no viruses or malware has been found, you may try opening the files.

WHAT IS A FRAUDULENT INVOICE?

Businesses are popular targets for invoice fraud. In these scams, criminals send bills for goods or services the business never ordered or received. The scam succeeds mainly because the invoices look legitimate and unsuspecting employees don't look closely to see it's not real. They simply make the payment, thinking someone else in their company placed the order. False invoice scams rake in billions of dollars every year.

PROTECT YOURSELF FROM INVOICE SCAMS

- Be cautious when processing invoices and ensure your accounts payable personnel are aware of the prevalence of these scams.
- Verify unfamiliar vendors and don't purchase from new suppliers until you confirm their credibility.
- Check invoices against original purchase orders to ensure there are no discrepancies.
- Don't rush to pay. Protect your company's assets by withholding payment until all info is verified.
- Check the company with the Better Business Bureau or State Attorney General's office.

WHAT THIS MEANS FOR COUNTIES

We recommend installing anti-virus and anti-malware and checking with a supervisor for authorization to copy data for use outside of the office. If you have had such data on a USB drive and are later giving it to someone else, make sure to do a secure wipe of the drive/media before giving it to them. It is also best practice to encrypt all data so it cannot be viewed if the media is lost.

County Technical Services, Inc.
Technical Updates are available online at ctsi.org
800 N Grant St, Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832