



Welcome to the TXDPS Cyber Security Newsletter

Seems like only yesterday, we were absolutely baking in the summer sun. Now Halloween looms!

1 big thing: October also brings Cybersecurity Awareness Month (CAM)



What to know: Cybersecurity Awareness Month is a collaboration between government and private industry to raise awareness about digital security and empower everyone to protect their personal data from digital forms of crime.

[The Cybersecurity and Infrastructure Agency \(CISA\)](#) and the [National Cybersecurity Alliance \(NCSA\)](#) partner to create resources and communications for organizations to talk to their employees and customers about staying safe online.

While most of the cybersecurity news articles are about massive data breaches and hackers, it can seem overwhelming and feel like you're powerless against it. But Cybersecurity Awareness Month reminds everyone that there are all kinds of ways to keep your data protected. It can make a huge difference even by practicing the basics of cybersecurity.

This year marks the 20th Cybersecurity Awareness Month campaign, CISA (along with NCSA) is celebrating with a new, year-round awareness campaign, *Secure Our World*.

[Secure Our World](#) is here to remind us that there are simple ways to protect yourself, your family and your business from online threats.

Cybersecurity Awareness Month 2023 and Secure Our World will focus on four key behaviors:

- [Use strong passwords](#) and a [password manager](#)
- [Turn on multifactor authentication](#)
- [Recognize and report phishing](#)
- [Update software](#)

For more information, ways to get involved, registrations for events and copies of research reports, head on over to [NCSA's website](#).

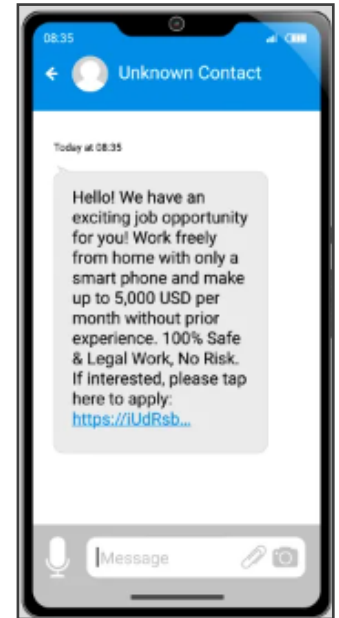
In the News

How social engineering takes advantage of your kindness

(Katie Malone | September 18, 2023)

MGM Resorts disclosed a massive systems issue that reportedly rendered slot machines, room keys and other critical devices inoperable. What elaborate methods were required to crack a nearly \$34 billion casino and hotel empire? According to the hackers themselves (and seemingly confirmed by a source speaking with Bloomberg), all it took was a ten minute phone call.

The alleged hackers behind the MGM issue, by all appearances, gained access through one of the most ubiquitous and low-tech vectors: a social engineering attack. Social engineering psychologically manipulates a target into doing what the attacker wants, or giving up information that they shouldn't – in this case, apparently, by pulling a fast one on an unsuspecting IT help desk worker. The consequences range from taking down global corporations to devastating the personal finances of unfortunate individual victims. But what makes social engineering attacks so effective, and why are they so hard to prevent?



It seems counterintuitive to hand over sensitive information to a complete stranger, but attackers have developed ways to trick you into feeling comfortable doing just that. Those could include building trust over time, gathering information about you to seem like they know you or using a sense of urgency to get you to act quickly without thinking through what you're giving up. That's why common personality traits among cyber victims include being extroverted, agreeable and open to new experiences, according to Erik Huffman, a researcher who studies the psychology behind cybersecurity trends.

"Fear is an attack vector. Helpfulness is an attack vector," Huffman said. "The more comfortable you are, the more hackable you become."

Read full story: <https://www.engadget.com/how-social-engineering-takes-advantage-of-your-kindness-170043531.html>

A Few More Cyber News Stories:

Amid MGM, Caesars Incidents, Attackers Focus on Luxury Hotels

<https://www.darkreading.com/cloud/mgm-caesars-incidents-attackers-luxury-hotels>

Millions of files with potentially sensitive information exposed online, researchers say

<https://cyberscoop.com/open-directories-exposed-files>

CISA rolls dice on public service campaign to raise cyber awareness

<https://www.cybersecuritydive.com/news/cisa-campaign-cyber-awareness/694920>

Clean Desk Check

This Month's Challenge


Let's see just how secure your work areas are as this month's cyber challenge!

Use this scorecard to see what's in your workplace. Be honest!

Take a stroll around your cubicle space or office (without looking like a creepy snooper) and check mark each item you notice. Then, add up your score!

Send me your scores, and let's see who has the cleanest (and most secure) work area!

WORKPLACE QUIZ



WHAT'S IN YOUR WORKPLACE?

To complete this quiz, take a walk around your workplace and put a check mark next to each item you notice. Each check is worth a specific number of points. Add up the points to reveal the level of physical security in your organization, at home, or wherever you are working remotely.

0 points = Place **OF** Protection

6-10 points = Dangerous Digs

1-5 points = Center for Concern

11 or more = Exposed Environment

1 POINT

- ☐ Desk littered with potential confidential information
- ☐ Calendar on display with important meeting dates
- ☐ Suspicious USB drive

5 POINTS

- ☐ Confidential files stored in an unlocked filing cabinet
- ☐ Unattended mobile device
- ☐ Forgotten key fob or ID badge

10 POINTS

- ☐ Login credentials written on a sticky note
- ☐ Whiteboard displaying past meeting notes
- ☐ Unlocked computer

-5 POINTS

- ☐ Privacy protectors on screens
- ☐ An employee who scans their badge despite walking in with a group
- ☐ Documents properly shredded before disposal
- ☐ Security cameras