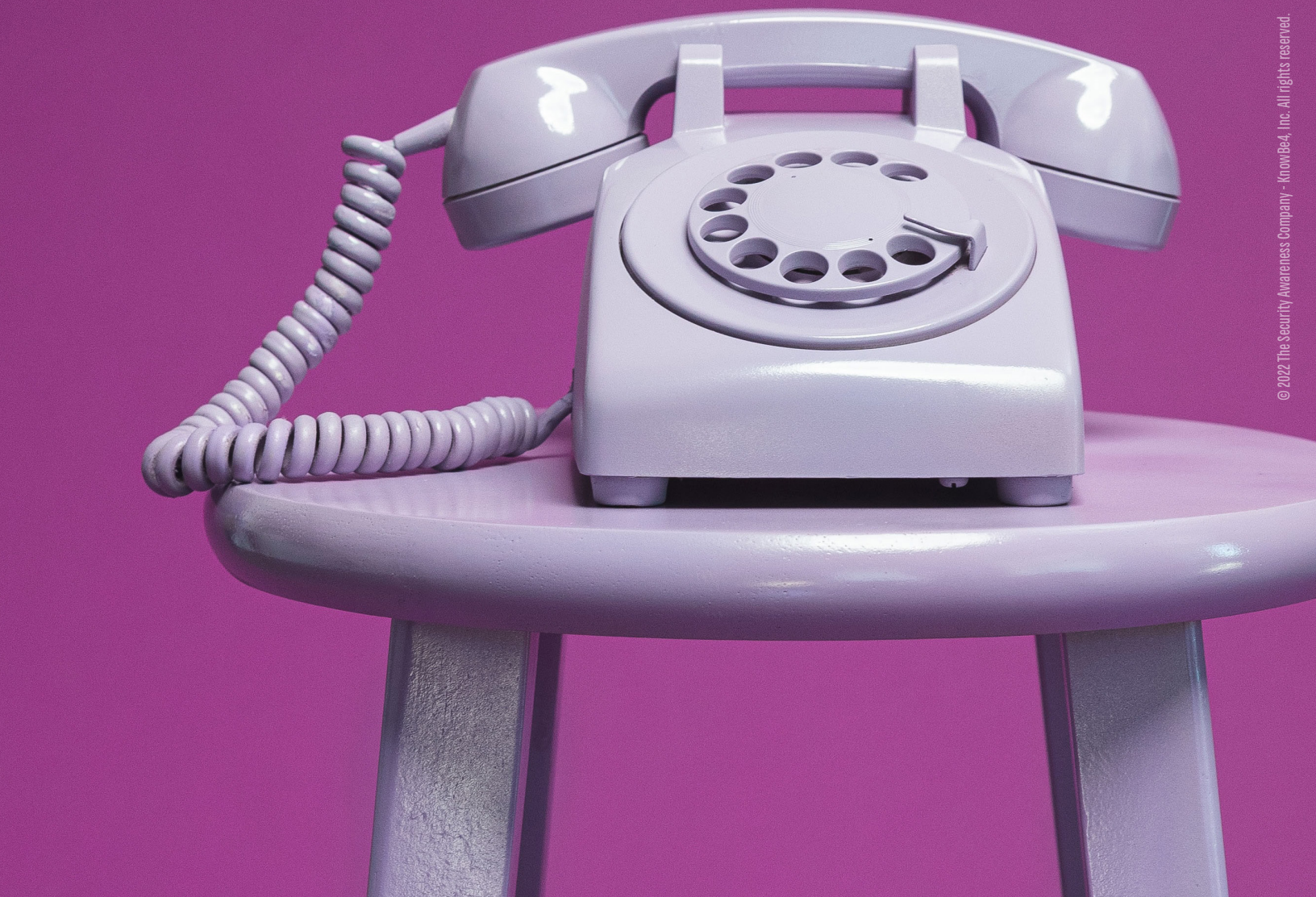
September 2022

# SecurityAwarenessNews

the security awareness newsletter for security aware people

# Incident Response

## Incident Response Plans Explained
## Incident Response and You
## Preventing Security Incidents



# Incident Response Plans *Explained*

Imagine you run your own organization. One of your employees falls for a phishing attack that leads to a malware infection. What would you do in this situation?

The goal of an incident response plan is to eliminate that very question. While it's obviously desirable to prevent security incidents, it's crucial that organizations have a plan in place for when unfortunate scenarios emerge.

***Let's explore this concept in more detail by answering a few common questions.***

## *What is an Incident Response Plan?*

An incident response plan serves as a play-by-play strategy an organization employs to help detect, respond to, and recover from security incidents. It's similar to emergency evacuation procedures that many public buildings implement.

## *Why is Incident Response so Important?*

Failing to prepare is preparing to fail. Incident response plans empower organizations to accurately and efficiently identify and recover from security incidents. Without a plan, it would be difficult to quickly mitigate damages.

## *What are the Steps of an Incident Response Plan?*

While every organization may have different structures and terminology, generic steps of most plans include:

1. **Preparation** – build a list of assets, and identify risks to those assets.
2. **Detection** – discover and analyze the security incident.
3. **Containment, eradication, and recovery** – contain the incident, remove the threat, and restore affected assets.
4. **Post-Incident Analysis** – determine how the incident occurred, and take measures to reduce the probability of similar incidents in the future.

## *What's Your Role Regarding Incident Response?*

An organization's incident response plan won't work unless employees report incidents as soon as they notice them. Your role, therefore, is to stay alert and report incidents immediately. The longer something goes unreported, the more damage it could cause.

## *Key takeaway:*

Incident response plans help organizations develop policies that prioritize the security of systems, data, and (most importantly) people.

# INCIDENT RESPONSE AND YOU

Incident response plans often include modern security solutions that help monitor for threats. However, even with the latest and greatest technology, incident response still heavily relies on people making smart decisions. Here's how you can help:

## Use situational awareness.

Situational awareness is a simple concept that focuses on staying alert for threats in both physical and digital environments. Take notice when something seems off, then take action to mitigate potential damages.

## Avoid assumptions.

Assumptions lead to mistakes. For example, just because an email appears to come from someone you know doesn't mean it's trustworthy. Assuming so could lead to a successful phishing attack. Remain skeptical and follow your instincts.

## Know how to report.

It's everyone's responsibility to know how to report suspicious events and to whom. If you need more information about how our organization handles incident reporting, please ask!

## Report immediately.

Remember, the longer an incident (or event) goes unreported, the more damage it could cause. If you see something, please say something as soon as possible. Timely reporting empowers organizations to quickly inspect what happened and implement corrective measures.

## Follow policy.

Policies are designed to keep confidential information confidential, and to maintain the privacy of employees, customers, and associates. By always following policy, you help ensure the continued success of our organization.

## Phishing Warning Signs Refresher

Given that phishing attacks are the most prevalent security event, make sure you stay alert for these common warning signs:

- **Poor grammar:** the email features misspellings or unusual wording
- **Urgent messaging:** the sender asks you to click on a link immediately
- **Threatening language:** the message claims, for example, that an account has been suspended
- **Generic greetings:** the sender fails to address you by name or username
- **Unrealistic promises:** the message says you've been awarded a significant amount of money

***Note:*** Although phishing typically happens via email, keep these warning signs in mind when handling text messages and other forms of communication. Always think before clicking!

# PREVENTING SECURITY INCIDENTS

What's the difference between a security event and a security incident?

A security event is any observable occurrence that could compromise an organization's security and threaten the integrity of infrastructure or data. A security incident is an event that results in negative consequences, such as a data breach or malware infection.

Why does this matter? Organizations encounter events daily. An employee receiving a phishing email qualifies as an event. It doesn't become an incident until someone clicks on a malicious link or downloads an attachment.

With that in mind, let's review a few examples of security events and what you can do to prevent them from becoming security incidents.

## PHISHING ATTACKS

Emails that contain malicious links or attachments are one of the most common types of cyberattacks. Always hover over links to reveal their true URL, don't click unless you can confirm the email is legitimate, and use extreme caution when handling attachments.

## MALICIOUS USB

Cybercriminals infect USB drives with malware and place them somewhere a curious worker might find them. When plugged in, the USB device infects the victim's computer. This security risk can be easily avoided by never using USB devices that you don't own, especially any you might find at random.

## OPEN DOORS

Many organizations require proper authorization and authentication to enter certain areas. So while a door left ajar might seem insignificant, it's not much different from someone sharing their password. Always ensure doors to secured areas remain closed and locked to prevent unauthorized access.

## SUSPICIOUS PHONE CALLS

Scammers can hide their identity over the phone and pretend to be someone else, such as a bank representative or a member of an organization's IT department. This tactic—known as vishing—is used to trick people into revealing confidential information. Never assume someone is who they claim to be.