July 2017

SecurityAwarenessNews

the security awareness newsletter for security aware people

See Something, Say Something!

Security Incidents & Where to Report Them

Incident Response IN ACTION & IN ALL THREE DOMAINS

PLUS: The Three Lives of Incident Response

Security Incidents & Where to Report Them

Most of our efforts in the battle against cybercrime are proactive and preventative by design. We work together and do everything we can to prevent an incident before it occurs. But what happens when those efforts fall short? When something goes wrong? When the conversation switches from, "It won't happen to us," to, "It happened to us, now what?" Most security professionals say, **"WHEN it happens to you... not if..."** It's this type of unfortunate scenario that gives life to our **"Hear something? See something? Say something!"** motto—a motto that applies to both proactive and reactive approaches to information security.

Security incidents are going to happen, sometimes because of mistakes and sometimes because of things beyond our control. What's important is how we handle them. If we don't report them—even those little things that seem unimportant—chances are they'll happen again. How we handle incidents is just as important as what we do to prevent them!

When you run across ANYTHING that could be a potential security incident—a phishing email, a suspicious package, an open door that's usually locked—you need to report it! Follow policy and make sure you know how to quickly report any security situation. If you have any questions at all about our reporting process, please ask! There are no stupid questions when it comes to our collective security.

SECURITY INCIDENT	RESPONSE
Receive a phishing email?	Report it so your teammates and co-workers can be alerted.
Notice someone not wearing a badge in an access-controlled area?	Kindly escort them to the proper location and alert a supervisor.
Receive a phishy phone call asking for private information?	Don't just hang up; make a detailed report and send it to the appropriate party.

OTHER USEFUL RESOURCES:

Cyberbullying

The Cyberbullying Research Center provides an unprecedented resource of where and how to report everything from social media to messaging apps. be sure to share this info with your friends and family: **http://cyberbullying.org/report**

Phishing

Report phishing attempts to the online service provider when applicable (such as Google, Apple, and Amazon). Forward phishing emails to **spam@uce.gov**, **reportphishing@antiphishing.org**, and **https://www.apwg.org/report-phishing/overview/**

ID Theft and Cybercrime

United States: **https://www.identitytheft.gov/#what-to-do-right-away** and **https://www.ic3.gov**

United Kingdom: **http://www.actionfraud.police.uk**

Europe: **http://ec.europa.eu/internal_market/fpeg/identity-theft_en.htm** and **https://www.europol.europa.eu/report-a-crime/report-cybercrime-online**

India: **http://cybercellmumbai.gov.in**

Australia: **https://www.acorn.gov.au**

South Africa: **https://www.safps.org.za**

Good security comes from timely response. Report security incidents immediately!

Incident Response *in Action*

What is Incident Response?

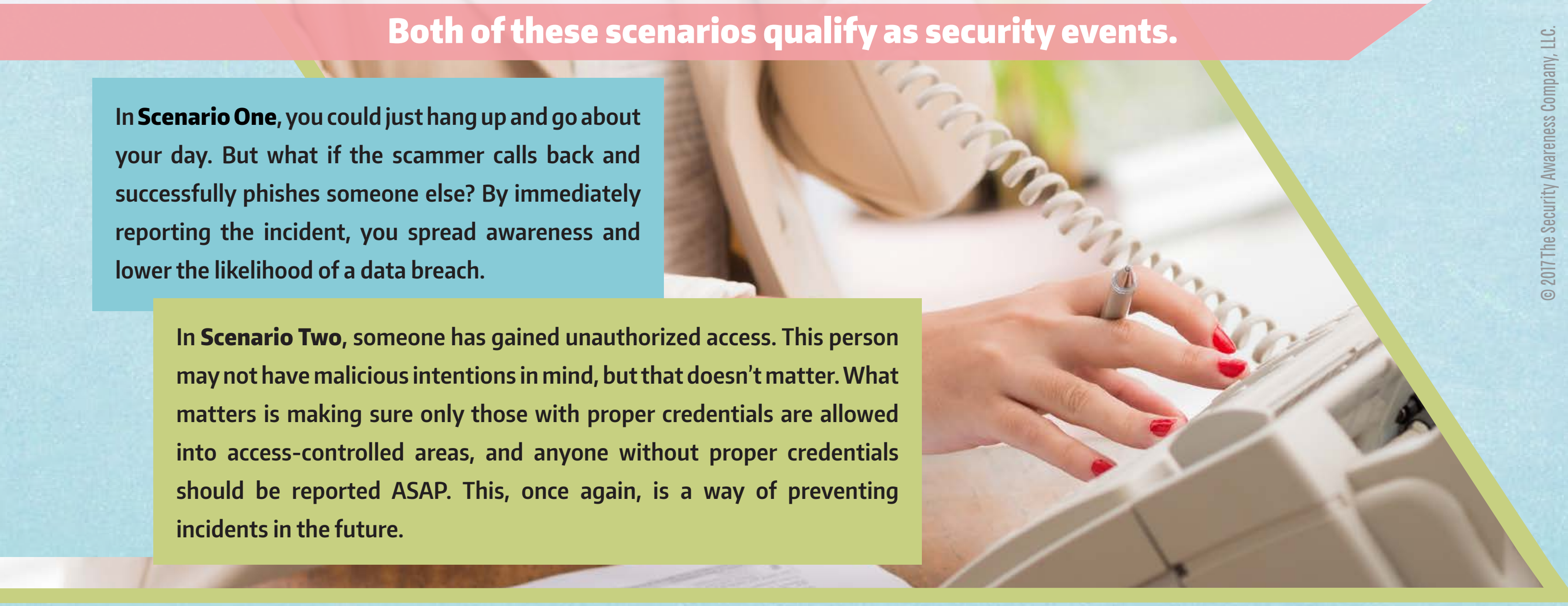
Incident response is the process of recognizing, identifying, and reporting a potential security incident to the appropriate party. Be sure to follow our incident response policy. ***If you're not sure, ask!***

Examples of Incident Response

Scenario One: You receive a phone call from someone claiming to be IT and needing your login credentials to upgrade your computer to the newest software. But, since you're a cyber-savvy person, you wonder why an IT Admin is breaking policy and asking for your password. Or, why they can't implement upgrades remotely without your help? *What do you do next?*

Scenario Two: While signing for a package in the lobby, you notice someone swipe their badge and enter the building. But there's just one problem -- this person doesn't notice that someone else slipped in behind them before the door could lock. *Now what?*

Both of these scenarios qualify as security events.



In **Scenario One**, you could just hang up and go about your day. But what if the scammer calls back and successfully phishes someone else? By immediately reporting the incident, you spread awareness and lower the likelihood of a data breach.

In **Scenario Two**, someone has gained unauthorized access. This person may not have malicious intentions in mind, but that doesn't matter. What matters is making sure only those with proper credentials are allowed into access-controlled areas, and anyone without proper credentials should be reported ASAP. This, once again, is a way of preventing incidents in the future.

Security Incident vs. Data Breach: What's the Difference?

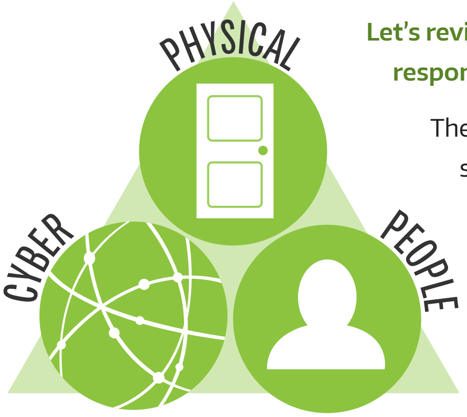
A **security incident** is when any cyber, human, or physical event potntially threatens the confidentiality, integrity or availability of our data or resources. That could mean a system being infected with malware. It could be website defacement. It could be an unauthorized person gaining access to somewhere they shouldn't be. It could mean being knocked offline by a distributed denial of service (DDoS) attack.

A **data breach**, on the other hand, is a severe security event where information such as passwords, identification numbers, trade secrets, intellectual property, or anything that falls under the PII (personally identifiable information) umbrella, is leaked.

Basically, all data breaches are security incidents but not all security incidents are data breaches. Regardless of definitions, they all need to be reported ASAP. *When in doubt, ask!*

Good security comes from timely response. Report security incidents immediately!

INCIDENT RESPONSE
IN ALL THREE DOMAINS



Let's revisit one of our favorite Triads – **the Domains: Cyber, Physical, Human** – and gauge our responsibilities for identifying and reporting incidents in each one.

The **Cyber Domain** covers everything from the internet to our networks, computers, and smart devices, as well as data, encryption and all things virtual.

The **Physical Domain** is the tangible side of security. It's our office buildings, desks, documents, badges, doors, locks, file cabinets, storage facilities and physical media. Some people include servers in this domain, too. As long as you're consistent, you'll be fine!

The **Human Domain** is where we interact with people—co-workers, suppliers, clients, and partners, as well as possible fraudsters, who impersonate legitimate people, a fake delivery guy, for example.

INCIDENTS TO REPORT IN...

THE CYBER DOMAIN

Phishing. Still the dominant method used by cybercriminals, phishing is the most common way malware finds its way onto computers and networks. According to the Verizon Data Breach Investigations Report, 66 percent of malware was installed via malicious attachments. Furthermore, the number of spam messages sent each day has reached 90 billion, according to Norton. While mostly harmless, excessive junk mail can overload servers and impact performance. If you are seeing an unusually high amount of spam don't hesitate to report it! This also includes SPIM (spam sent via instant messaging), and SPIT (spam sent over Internet Telephony).

Smishing. Like phishing, smishing is a social engineering attack using text messaging to deliver bogus links. Be on the lookout for odd requests that come to your device, and never click unless you're absolutely sure it's legit. In most cases, it's safe to assume the link is malicious.

Privileged Access. One of the keys to information security is protecting our systems from unauthorized access. This is why we have access controls in place, which means certain people are granted certain permissions. It's important to never give your login credentials to anyone, and if you feel you've been given access to information unnecessarily, don't be afraid to say something!

THE PHYSICAL DOMAIN

Tailgating. When someone sneaks into a secured area or checkpoint by following someone else who has legitimate access, they are tailgating. Unauthorized, physical access is a security risk that needs to be reported immediately.

Piggybacking. Similar to tailgating, someone piggybacks by gaining access via someone else's credentials. The biggest difference is the person with legit access knowingly allows this person in. For example, if you swipe your badge and hold the door open for someone, you've just allowed them to piggyback...and you've created a security event!

Malicious media. The temptation to plug in a random USB or optical disc, such as one found on the ground or received at random through the mail, is exactly what social engineers bet on when they load these things with malware. USBs are especially risky since many are programmed to auto-run, which can infect a computer just by being plugged in!

THE HUMAN DOMAIN

Vishing. The telephone equivalent of phishing, vishing is a scam whereby the attacker attempts to convince someone to relinquish sensitive information over the phone. This is often carried out with automated messages that inform the victim there has been suspicious activity on their bank account (for example), and advises them to call a specific number or respond over keypad.

In-person pretexting. Most scams include some version of a pretext—a made up scenario that targets people in hopes of tricking them into divulging sensitive info. In-person pretexting happens live, putting you face-to-face with a social engineer. Think wedding crashers and apply it to sensitive information. Is the FedEx guy really FedEx? Or the water or telephone repair-person?

Disgruntled employees. This is a tough one because it could involve a co-worker you know on a personal level. Disgruntled employees threaten both cyber and physical safety! We're not asking you to be a "tattletale," but if you see someone acting erratically or suspiciously, report them immediately.

STRANGERS IN THE HALLS? NO BADGE? QUESTION THEM! Don't go all Bruce Willis on them, but politely ask who/what/where/why etc. Most likely, it's just an oops! Make sure your badge-ID policy is consistent with how to handle and report people wandering around your facilities.

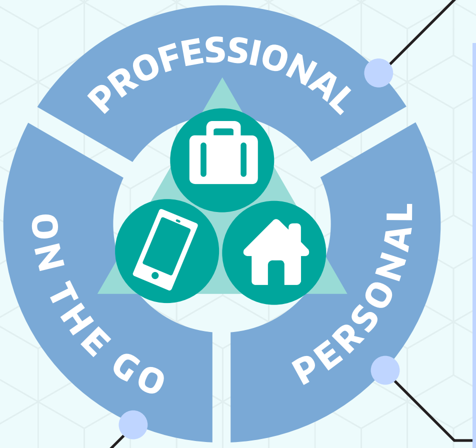
Good security comes from timely response. Report security incidents immediately!

The 3 Lives of Incident Response

The overlapping of security in our professional, personal, and mobile lives accentuates the need for situational awareness. It also means that our mindset must be to respond to security events regardless of where we are or what we're doing. The Many Lives Triad harnesses that sentiment by focusing on the threats we face in each.

It's important to understand the power you have here at work. **The data and resources you have access to puts a great deal of responsibility on your shoulders** to ensure that it stays confidential and doesn't end up in the wrong hands. But it also means speaking up when something isn't quite right, even if it was just a mistake and not a hostility. The sooner you respond, the sooner we can recover, ultimately mitigating further damage.

Our mobile lives involve even more threats, as it's not just cyber-attacks we need to worry about! We must be aware of our physical surroundings, keeping our devices out of plain sight when accessing sensitive information, and keeping them in our possession at all times. By staying abreast of the threats we face, we can eliminate incidents and have nothing to report! **Make sure you know what you would do if you lost your work phone, or broke your personal laptop.** How would you remediate a stolen purse or briefcase containing devices, credit cards, and thumb drives?



You have to follow policy at work. But what about at home? Do you encourage your family and friends to lookout for phishing scams? If you have kids, do they know who to tell if they witness cyberbullying or inappropriate activity in chat rooms or on social media? What's your family policy for backing up photos, tax documents, and medical records? **Keep in mind security incidents go well beyond cybercriminals attacking large organizations!** How do you keep your neighbors from connecting to your home WiFi? Do you use an easy-to-guess password for your Netflix account? What about your bank accounts? A security incident can be ANYTHING related to the security and privacy of your personal data, home networks, and devices.

We all (should) have fire alarms and a fire evacuation plan in case of an incident at home, and we all should have a security incident remediation and prevention plan as well!

It's easy to see the overlap between the three lives of security and how they work together. How often do you access work stuff from home or personal stuff from work? And how often do we access both while mobile? *Though the threats we face vary in each circumstance, we should treat them the same.* Meaning we should be familiar with them and have a plan in place to react when security incidents present themselves.

Security Awareness at Home

While your job as a cyber-aware employee is to stay alert and ensure the information you access remains private, we encourage everyone to take that part of work home with them. Developing a home security policy is the best way to keep your household safe from cyber threats like malware and identity theft. If you're interested in developing a cybersecurity policy at home, follow these seven steps!

▶ ▶ ▶ ▶ ▶ ▶ ▶ http://secaware.co/2qUyoTf

Good security comes from timely response. Report security incidents immediately!