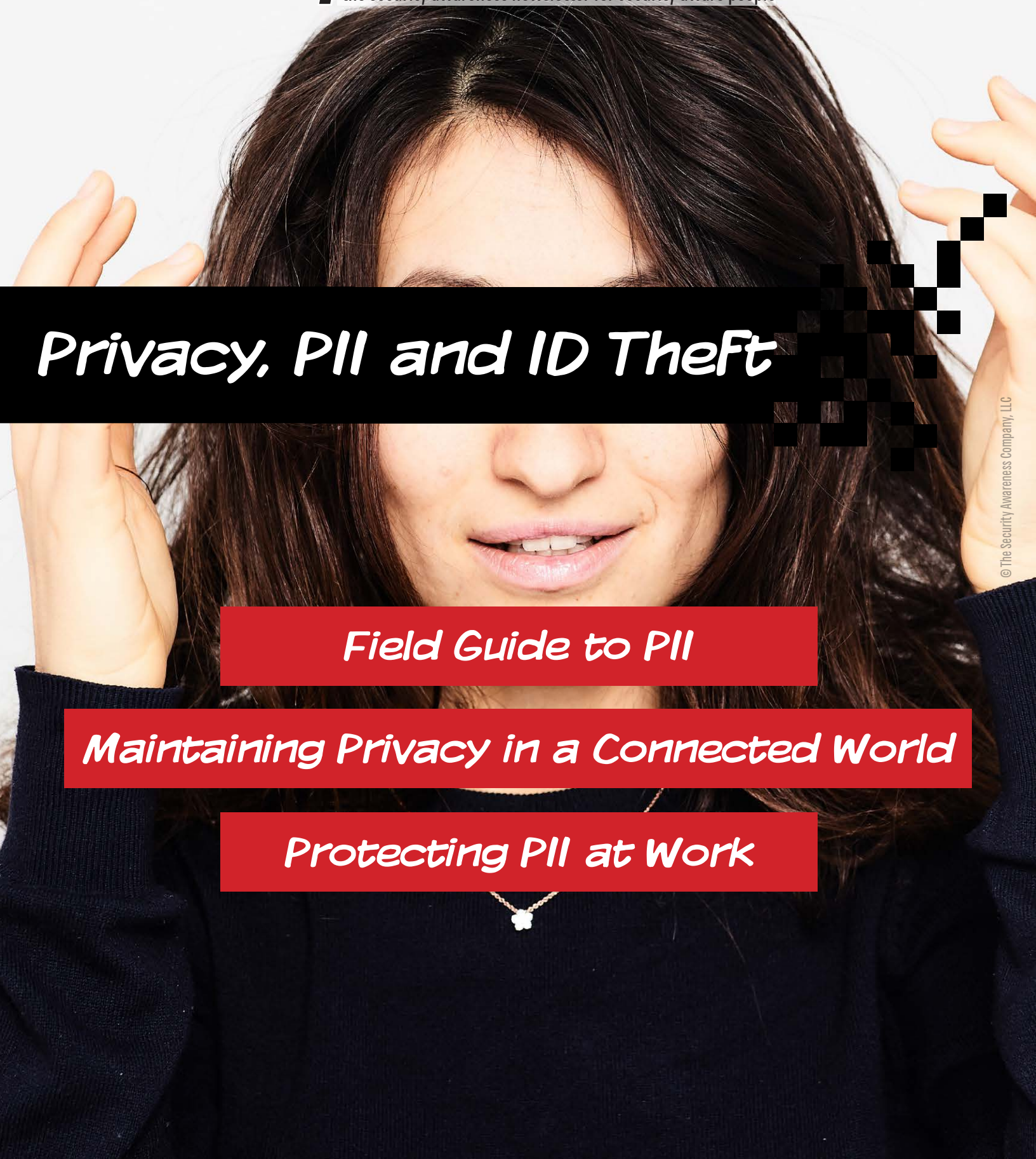
April 2019

Security Awareness News

the security awareness newsletter for security aware people



Privacy, PII and ID Theft

Field Guide to PII

Maintaining Privacy in a Connected World

Protecting PII at Work

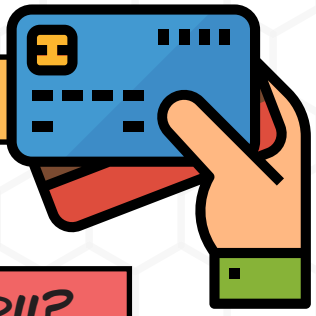
Field Guide to PII

Whether at work, at home, or on the go, we're beholden to a lifecycle of data that is often the top target of cybercriminals. Protecting that data isn't a highly technical process, but rather one that requires common sense and a strong commitment to privacy in every aspect our lives!

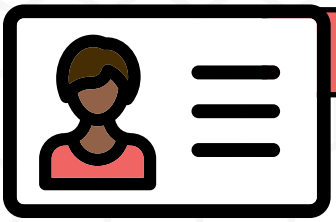
What is PII?

PII, or personally identifiable information, is sensitive data that could be used to identify, contact, or locate an individual.

What are some examples of PII?



PII includes *(but is not limited to)* home addresses, personal email addresses, national ID numbers, credit card numbers, and personal phone numbers.

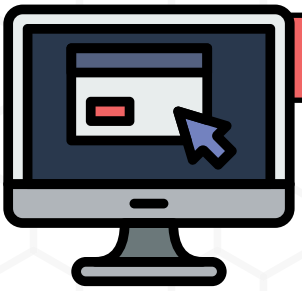


What are some examples of non-PII?

Info such as business phone numbers and email addresses, race, religion, gender, workplace, and job titles are typically not considered PII. But they should still be treated as sensitive, linkable info because they could identify an individual when combined with other data.

Why is PII so important?

On a personal level, our PII is necessary to acquire some goods and services, such as medical care and utilities. But in the wrong hands, PII leads to identity theft and other forms of fraud. On a professional level, we may store PII of customers, clients, vendors, contractors, employees, and partners. If left unprotected, our organization could face steep fines and our reputation could be severely damaged.



How do you protect PII at work?

Protecting PII begins and ends with following our organization's security policies, which were created to ensure that the data we handle remains private. Treat all requests for sensitive info with a high degree of scrutiny, stay alert, think before you click, and if you have any questions, please ask!

How do you protect PII at home?

We encourage you to develop a home security policy similar to what we use here at work, which calls for common sense practices, such as not clicking on random links and attachments, guarding personal info online *and* in real life, destroying sensitive documents beyond recognition, and setting social media profiles to fully private.

Maintaining Privacy in a Connected World

Living in a society that's so immersed in connectivity and technology has, unfortunately, led to a sacrifice of privacy. Certain smartphone apps, for example, can't function without access to our contacts and location. If you need medical care, you must entrust your highly sensitive info to an entity that you *know* is a common target for cybercriminals. And every smart gadget you activate in your personal life collects, stores, and transfers your data in exchange for a bit of convenience. But at what cost?

Our data is like currency, and it has value for both legit and illegal purposes. Preventing the latter should remain our top goal. How do we accomplish that goal? By using the best defense we have: common sense. Scammers and social engineers violate privacy by gaining your trust and convincing you to release info or to click on something or to install something. **Stay alert, follow policy at work, and prioritize security at home!**

Avoiding Identity Theft in 5 Easy Steps

1. **Reduce information.** Limit the amount of personal info you make public. Set your social media profiles to fully private and thoroughly vet all friend requests.
2. **Remain skeptical.** Government and tax entities will never email you requests for payments. Treat all requests for sensitive info or money with a high degree of skepticism.
3. **Respond responsibly.** If you receive a notification that an account has been compromised, call the number on your card or visit the legit website. Never click on unsolicited links that come via emails or text messages.
4. **Record activity.** Log into your financial accounts weekly to confirm that no unauthorized purchases have been made and consider placing fraud alerts on your credit reports.
5. **Restore defaults.** When recycling old smart devices, be sure to delete all data and restore to factory default. Shred all sensitive documents before discarding.

Data Breaches at Work

While all of this is great info to help with recovery, we need ***your*** help with prevention by ensuring that our clients, customers, and partners (and your co-workers!) never experience this scenario. That's why we ask you to stay alert and follow our policies. ***Data breaches impact all of us!***

What do you do if you're part of a data breach?

Perhaps no email is worse than the one that begins with something like "Dear customer, we regret to notify you of a data security incident that may have exposed some of your personal information…" Regardless of how the incident occurred, your next actions are an imperative part of recovery. Here's a quick, step-by-step guide for what to do if your data is part of a breach.

Update your passwords. Hopefully, you already use unique codes for each account, but a breach serves as a good time to update your passwords.

Alert financial institutions and credit bureaus. By reporting the incident to the relevant institutions, you can mitigate future damages and prevent cybercriminals from making fraudulent charges or stealing your identity.

Place fraud alerts on your credit reports. In some cases, the compromised entity may offer free credit monitoring, which alerts you to any changes on your credit (such as a newly opened account). You can even take this a step further by freezing your reports, which prevents all credit checks until the freeze is lifted.

Keep a close eye on your banking accounts. It's important to routinely check for unauthorized transactions in general, but it is *essential* to do so after a data breach.

Stay alert for additional phishing attacks. Cyber thieves use stolen account credentials to launch phishing campaigns and other attempts to scam data breach victims.


Protecting PII at Work


As with every organization, job functions vary by department, but we all share one common responsibility: protecting the private data of our clients, customers, partners, and co-workers. This starts with following policy and ends with utilizing non-technical security awareness, such as keeping your workspace tidy (both physically and digitally), ensuring secured areas stay locked, and reporting all security incidents ASAP.

COMMON CAUSES OF DATA BREACHES

PHISHING ATTACKS

Phishing still ranks as the top reason data breaches happen. Think before you click!

WEAK PASSWORD PRACTICES

Attackers who gain unauthorized access to accounts can infiltrate organizations and steal info, or launch *additional* social engineering attacks. That's why it's vital that we utilize strong, unique passwords or passphrases for every single account.

UNPATCHED AND OUT-OF-DATE SYSTEMS

Leaving software and firmware outdated invites risk. Developers release updates to fix security patches and reduce vulnerabilities.

IMPROPER CONFIGURATIONS

A network with improper security configurations can easily be infiltrated.

SOCIAL ENGINEERING

Beyond phishing, social engineering also involves attempts at physically accessing buildings or contacting business phone numbers in hopes of scamming employees over the phone.

CIRCUMVENTING POLICY

Whether intentionally or accidentally, failure to adhere to organizational security policies leads to data leaks.

What do all of these have in common? Human error! Most security breaches are made possible by mistakes that individuals make and not by highly technical attacks. We remind you of this simply to highlight the role you play as a human firewall. Only **you** can prevent data breaches!

PHISHING REFRESHER

YOU MIGHT BE GETTING PHISHED IF…

- **The email contains incorrect spelling and bad grammar.**
- **The email begs you to click on a link or download a random attachment.**
- **The email features a sense of urgency or threatening language.**
- **The email comes from your boss…**

Wait, what?

An email **from your boss** could be a phishing attack? That's right! Not every phishing attack comes full of obvious red flags. Some utilize compromised or spoofed email accounts of executives to send requests for money or sensitive data to other employees. Known as CEO Fraud or BEC (business email compromise) this scam is common, dangerous, and gives you even more reasons to remain skeptical at all times.