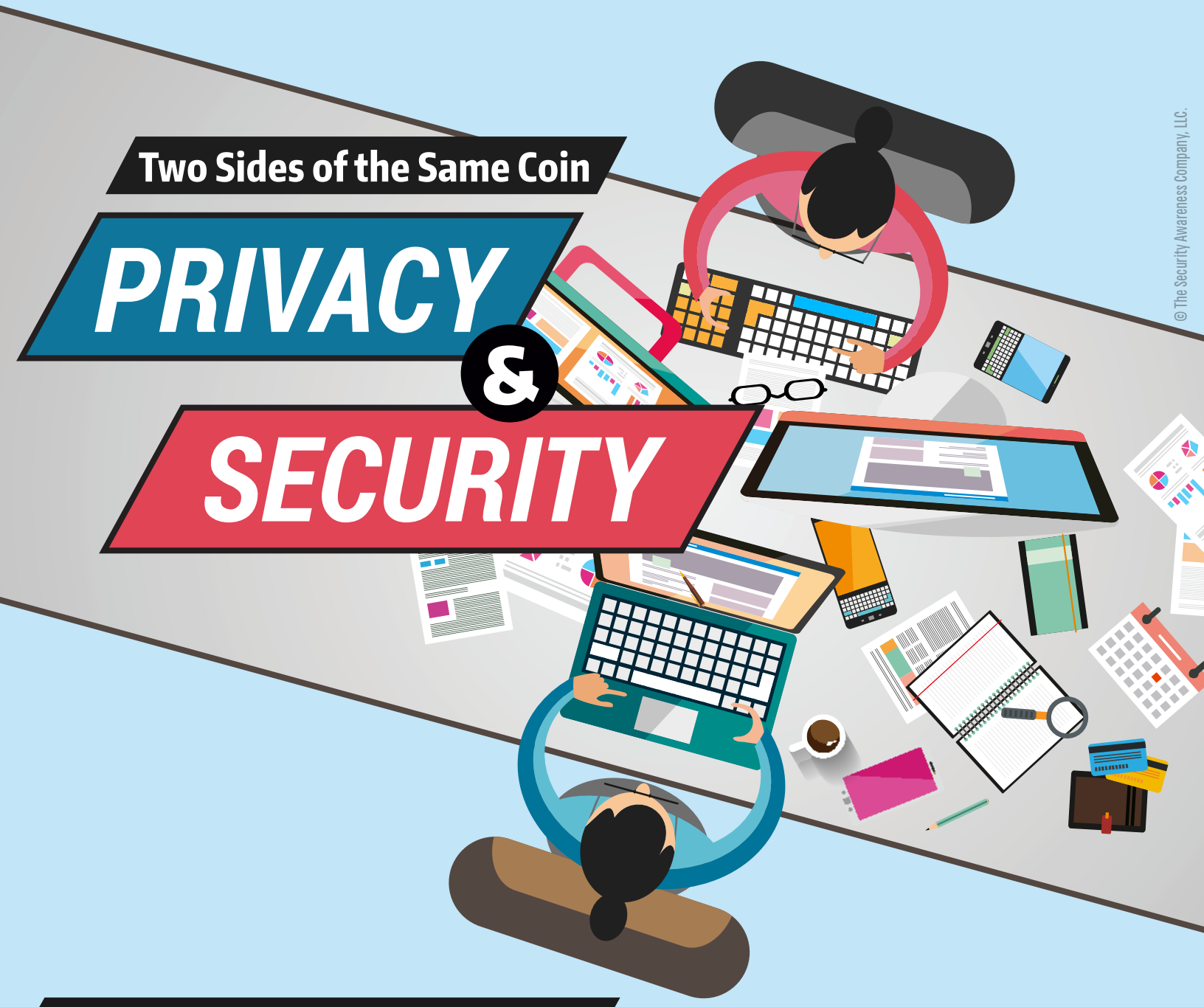
December 2017

Security Awareness News

the security awareness newsletter for security aware people



Two Sides of the Same Coin

PRIVACY & SECURITY

WHY COMPLIANCE MATTERS

UNDERSTANDING INSIDER THREATS

Privacy and Security

Two Sides of the Same Coin

Privacy and security work together, and often get interchanged in casual conversation. But there is a difference, and it's important to understand that difference.

Privacy refers to the appropriate use of any data that is collected, stored, and transmitted. "Appropriate" is the operative word here. When a customer or business client shares sensitive data with us, it is our duty to ensure we only use that data for its intended purpose. We are not, for example, going to send it to an unauthorized party or post it on Facebook.

Security refers to our efforts as Human Firewalls to ensure that data is not accessed by unauthorized parties, such as social engineers and cybercriminals. Security means not clicking on random links and attachments, making sure that our workstations are organized and password-protected, and verifying that access-controlled areas remain locked.

Think of it this way: privacy is often mandated by compliance regulations and organizational policies, while security is a measure of human and technical defensive solutions. While completely different, the two work together to achieve one common goal: guaranteeing the confidentiality, integrity, and availability of sensitive information at all times, at every level, no matter what.

If you ever question your role when it comes to privacy and security, or what our organizational policies are, please ask!

Cybersecurity and information security policies are put in place to ensure data privacy, much in the same way that a security system protects the privacy of your home. Data *security* comes down to the confidentiality, availability, and integrity of data, whereas data *privacy* concerns the appropriate use of that data.

"To me, the most frustrating thing is when people treat privacy and security as if they are trade-offs."
- Michael Chertoff, former Security of Homeland Security

"We don't have to make a trade-off between security and privacy. I think technology gives us the ability to have both."
- John Poindexter, retired US naval officer and Department of Defense official

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."
- David Brin , American scientist and sci fi author

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

UNDERSTANDING INSIDER THREATS

Do you consider yourself a threat to our organization? You probably don't, especially since we do our best to work together to form an alliance of strong, security-savvy individuals! Unfortunately, insider threats exist in every organization, from the CEO on down. So what exactly is an insider threat? Simple: anyone who has been granted access – from sensitive data to controlled rooms and buildings – is an insider threat. Why? Because they have access, and access requires responsibility.

THREE TYPES OF INSIDER THREATS

ACCIDENTAL

Oops, I sent sensitive information to the wrong person!

NEGLIGENT

I know it's against policy to access information from my personal device, but I'm going to do it anyway so I can work from home.

MALICIOUS

I wonder how much money I could make off this private information I have access to...

WHAT CAN YOU DO TO MITIGATE THE THREAT YOU OR OTHERS POSE?

Always follow policy.
Report all incidents.
Stay alert.
Respect privileged access.
Lead by example.

OFFBOARDING FROM 3 DIFFERENT PERSPECTIVES

When the time comes to move on from an organization, whether voluntarily or otherwise, we all play a role in making that a smooth transition for everyone involved. This process is known as **offboarding**.

OFFBOARDING FOR MANAGERS & EXECUTIVES

Your job is to ensure all departments know of the employee's departure, and that the transfer of responsibilities and data is organized in a way that benefits everyone. Organization is key to protecting information in both the physical and cyber domains, so it's vital that you have a detailed offboarding plan in place.

OFFBOARDING FOR I.T.

I.T. must update the employee's access to systems and networks immediately upon departure. That means changing logins and passwords, removing access to physical and cyber locations where necessary, and recovering organization-issued devices.

OFFBOARDING FOR THE DEPARTING EMPLOYEE

Regardless of reasoning, your role in departing from an organization is important! From training your replacement or co-workers to turning in property that belongs to the organization, you not only assist in protecting sensitive information, but also in fulfilling your role as a strong Human Firewall.

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

Why Does Compliance Matter?

When you make an online purchase, you provide banking information, your address, and other bits of PII (personally identifiable information). What if that data fell into the wrong hands? Who protects it, and what penalties exist for inadequate data practices?

Enter compliance regulations. They exist to protect sensitive information across multiple industries. Think about how many times you provide your full name, address, phone number, national ID number, and more. Whether you're setting up a new utility account or visiting a doctor, PII is a necessary part of doing business. This is why compliance regulations exist: to protect your PII no matter who has it or where it goes.

LET'S TAKE A LOOK AT A FEW COMMON REGULATIONS

HIPAA

Health Insurance Portability and Accountability Act

Goal: To keep medical information confidential and private, ensuring that it's only used in the way for which it is intended. This means that medical information can only be collected, shared, stored, and used for legitimate purposes and must be properly protected. HIPAA was signed into law in 1996. HIPAA is not just for doctors or medical professionals! Find out how HIPAA impacts your job function: http://secaware.co/NotADoctor.

PCI-DSS

Payment Card Industry Data Security Standard

Goal: To prevent credit card fraud and theft by implementing standards for vendors who process credit or debit information. PCI-DSS specifies 12 requirements for compliance, which are organized into six control objectives. Learn more about PCI, what you need to know, and common myths about the requirements: http://secaware.co/PCIFAQsMyths

GDPR

General Data Protection Regulation

Goal: To protect the privacy of all European Union residents, regardless of where their private information gets used or accessed. Organizations worldwide must be GDPR compliant in order to process, store, or transmit data of EU citizens. GDPR sets the gold standard for cross-border data regulations. Learn more about the global impact: http://secaware.co/GDPRImpact

PHI • *Protected Health Information* · any information regarding health status, health care, or payment for health care.

PII • *Personally Identifiable Information* · any information that can be used to identify an individual, such as national ID number, full address, phone number, date of birth, etc.

What is your role within our organization regarding compliance regulations? To know and always follow policy. Treat sensitive data with the utmost care, and keep in mind that data is not just numbers; it represents people. If you're not sure about our organization's policies or what regulations you must follow, please ask!

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

BONUS STAGE

The Battle Against ID Theft

According to a study conducted by Javelin Strategy & Research, identity theft cost consumers more than $16 billion/€13.6 billion last year. That number is on pace to be shattered this year, especially after the massive data breach reported by Equifax that impacted over 145 million people (and counting). Personally identifiable information (PII) is a hot commodity and continues to be the most sought-after data by cybercriminals.

(Source: https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html)

Why Do Cybercriminals Want Your PII?

Every day we create 2.5 quintillion bytes of data; enough to fill 10 million Blu-ray discs. A lot of that data is personally identifiable information and has more value than ever before.

If someone has your PII, they can pretend to be you. Health records give cybercriminals enough information to open credit card accounts on your behalf. They can take out a mortgage or use your medical info to file fake claims with insurers. Your information is the key that unlocks a very profitable door.

This is why it's critical for us all to know what information should be kept private. Here at work, if you handle customers' PII, know and follow organization policy to protect the confidentiality of their private data. At home, mind where you store PII and what you share. Monitor your online life, from medical records to financial files, from government records to eBay transactions. What you share online can, and will, be used against you. **It takes just one click to compromise the sensitive data of our customers, clients, business partners, co-workers, families, and yourself.**

A few examples of PII:

- **Full names**
- **National ID numbers**
- **Driver's license numbers**
- **Credit card numbers**
- **Date and place of birth**
- **Criminal records**
- **Country, state, or city of residence**

5 STEPS TO TAKE IMMEDIATELY IF YOU FALL VICTIM TO ID THEFT

STEP 1: CHANGE YOUR PASSWORDS

No surprise here! Changing your usernames and passwords, particularly those that protect banking accounts, is imperative.

STEP 2: CONTACT YOUR BANKS AND CREDIT CARD COMPANIES

Most credit card companies have a zero-liability policy, protecting consumers from fraudulent charges. Contact them immediately to freeze cards that may have been compromised.

STEP 3: PLACE A FRAUD ALERT ON YOUR CREDIT REPORT

By placing a fraud alert, you prevent cybercriminals from opening accounts in your name. Here is the contact information for the three major credit reporting agencies:

> *Equifax Fraud Department – 1-800-525-6285*
>
> *Experian Fraud Department – 1-888-397-3742*
>
> *TransUnion Fraud Department – 1-800-680-7289*

You can also place a freeze on your credit. Visit the FTC's website to see credit freeze FAQs. Wikipedia has a list of worldwide credit bureaus here: wikipedia.org/wiki/Credit_bureau.

STEP 4: LIVE IN THE U.S.? CONTACT THE FTC

The Federal Trade Commission has an entire website dedicated to reporting ID theft and getting a recovery plan: www.identitytheft.gov
You can use this form to file your report: www.identitytheft.gov/Assistant# and then follow these steps towards recovery: www.identitytheft.gov/Steps. Alternatively, contact your local police department to file a report.

STEP 5: NOTIFY OTHER INSTITUTIONS

Your identity could be used to open utility service accounts like cable or electricity. In the case of tax ID theft, the crook may attempt to file a fraudulent tax return. Placing fraud alerts and credit freezes will help eliminate some of these issues, but you may still need to contact insurance and utility companies to alert them that your ID has been compromised.

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