UNDERSTANDING THE ATTACKERS

In a lot of cases, knowing the ***why*** proves just as valuable as knowing the ***how***. If you've ever watched or read crime dramas, then you understand the word "intent." Investigators usually spend a lot of early efforts on solving the intent of a crime. Why was the crime committed? What was the motive? Understanding the **why** opens the door to serving justice. When it comes to security, understanding criminal motives has a direct impact on what we protect and how we do it.

WHAT — Personally Identifiable Information

Known simply as PII, this data includes a long list of items that can specifically identify an individual, such as full names, home addresses, and national ID numbers (to name a few).

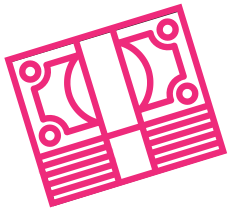
WHY — ID Theft

Identity theft ranks near the top as one of the most common crimes worldwide. By stealing your ID, criminals can act in your name. They can leverage your credit score to open accounts, file fraudulent insurance claims, and basically do anything you can do with your information. Here are five ways to prevent this from happening: https://www.thesecurityawarenesscompany.com/2017/03/23/five-ways-prevent-identity-theft/

WHAT — Usernames and Passwords (Online Accounts)

Although login credentials fall under the PII umbrella, criminals want them for more than just ID theft. Your usernames and passwords unlock a world of opportunity.

WHY — Cash



Gaining unauthorized access to any account, like email or social media, may lead to gaining access to other, more important accounts such as banks and credit cards. In this situation, the attacker can steal directly from you, or even sell your information on the dark web.

WHAT — Usernames and Passwords (Internet of Things)

Everything we connect to the internet, from routers to dishwashers (Internet of Things), opens another door for criminals.

WHY — DDoS Attacks

Distributed denial-of-service (DDos) attacks take down major servers by flooding them with more "hits" than they can handle. The results crash the servers and destroy all internet traffic that goes through them for extended periods of time. The easiest way to launch a DDoS attack stems from hacking smart devices, turning them into a botnet—tens of thousands of compromised devices used as an army. Botnets are often made possible by lax security settings of smart devices, especially default usernames and passwords.

WHAT — Email Addresses

Also considered PII, email addresses by themselves may not seem all that threatening. But when criminals gather thousands of them, the results can lead to disaster.

WHY — Phishing Campaigns

Phishing is the most successful social engineering tactic to date. Phishers launch campaigns aimed at specific companies or people (known as spear phishing) in hopes of spreading dangerous Trojans such as ransomware or other forms of malicious software.