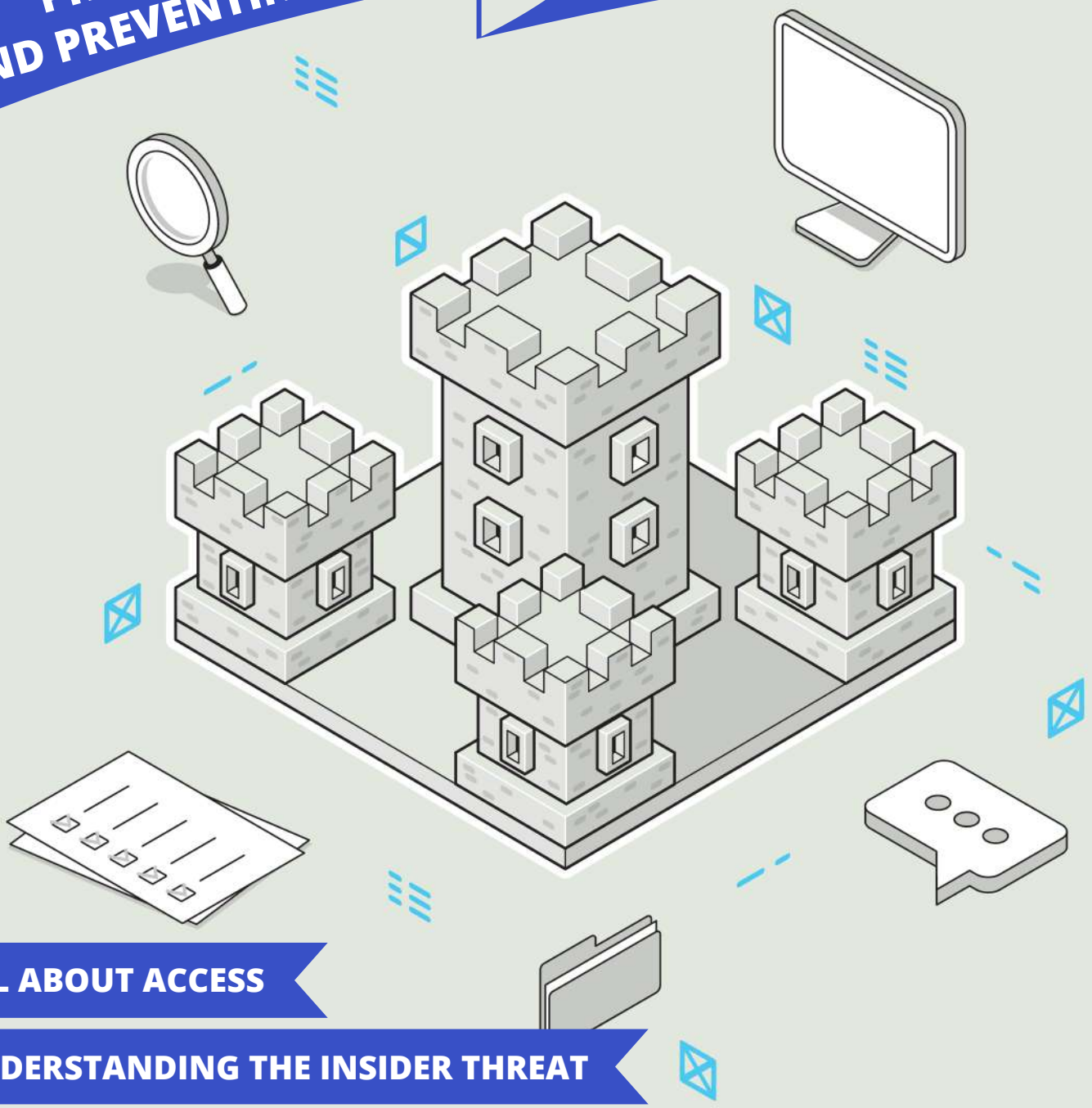
SecurityAwarenessNews

the security awareness newsletter for security aware people

PROTECTING DATA AND PREVENTING BREACHES



ALL ABOUT ACCESS

UNDERSTANDING THE INSIDER THREAT

THE LAST LINE OF DEFENSE

ALL ABOUT ACCESS

The flow of information begins and ends with access to information. This also means that information security flows through individuals (people like you) and the access they've been granted.

Every member of every organization has some level of access rights—the right to enter an office, to use a computer, to join a network, to view a database of confidential information. The higher level of access you have, the greater your responsibility.

What is access control?

Access control is a layered approach to the creation and management of user accounts within an organization. Just like there's a chain of command starting with executives and working downward, access to information and systems also has a chain of command, ranging from low-level accounts (such as a standard email address) to high-level accounts (such as IT administrators). Access control policies exist to minimize the risks posed by cyberattacks and human error, while still allowing employees to do their jobs.

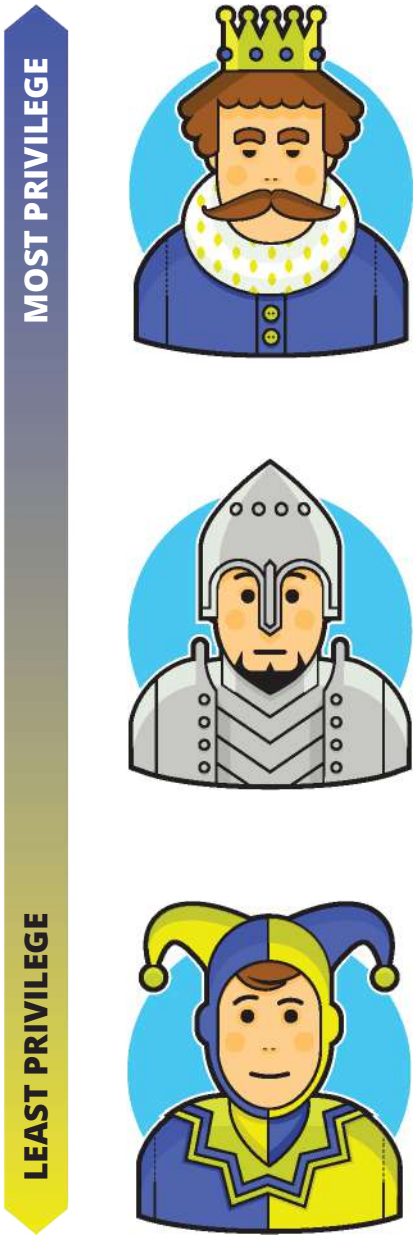
What is the principle of least privilege?

The principle of least privilege simply means that an individual will be given the minimal amount of access necessary to perform their duties. This process helps isolate and mitigate security breaches, effectively limiting potential damages.

What is your role in protecting access?

Remember that the access entrusted to you belongs to you, and you alone. Don't share your login credentials, don't allow someone to use your badge or keycards to enter secured areas, and protect every account with a strong, unique password. When working away from the office, store work-issued devices in a secure location so they won't be misplaced or get stolen.

In simple terms, protecting access involves a combination of technical controls and security-aware employees who understand and always follow organizational policies. If you need more information about this or if you have any questions, please ask!



UNDERSTANDING THE INSIDER THREAT

There's a direct correlation between having access to confidential data and being a threat to the security of that data. This correlation creates the concept of the insider threat, defined as "any individual who has access to an organization's data, networks, computers, and information." Insider threats fall into two general categories:

Malicious Insider Threats

Individuals who intentionally cause harm to an organization.

Accidental Insider Threats

Individuals who unintentionally cause harm to an organization.

The Malicious Insider

An executive assistant at a soft drink company stole documents of trade secrets and product samples with the intent to sell them to a competitor for a significant amount of money. Had the assistant been successful, the soft drink company would have lost their competitive advantage in the marketplace, endangering their long-term success.

The Accidental Insider

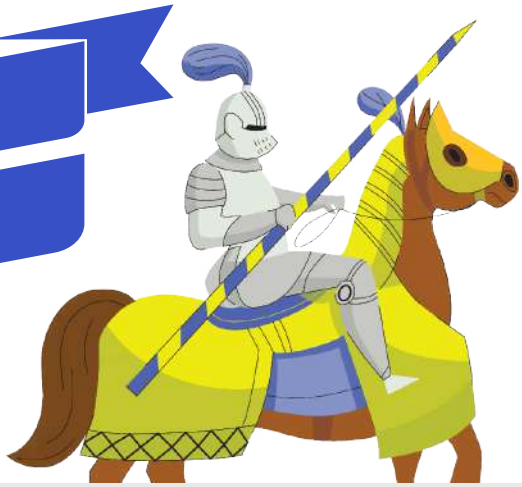
A customer service specialist accidentally emailed their spouse a spreadsheet containing confidential information of thousands of customers. Even though the spouse agreed to immediately delete the spreadsheet, the organization still had no choice but to inform their customers of the incident and offer credit monitoring services for free, resulting in a loss of revenue and a damaged reputation.

Both examples demonstrate that data breaches and other security incidents don't always involve criminal hackers attacking organizations. In fact, a recent study by Stanford University found that 88% of data breaches were the result of human error, which is why insider threats represent a major concern.

So you're an insider threat; now what? Become an insider asset! Here's how:

- ***Respect your access.*** As previously mentioned, never share your passwords or keycards/badges with anyone, and lock your workstation when not in use.
- ***Think before you click.*** Cybercriminals use malicious links or attachments to spread malware that steals data and account credentials.
- ***Verify the source.*** Always make sure confidential information is only shared with the proper, authorized parties.

THE LAST LINE OF DEFENSE



When a data breach occurs, it's tempting to place the blame on external attackers or to assume it was the result of a broken system or poor coding. But consider the following quote from Bruce Schneier, a well-known security technologist:

"Amateurs hack systems; professionals hack people."

That quote highlights one of the most important concepts of cybersecurity: it's a people problem, not a technology problem. A cybercriminal's path of least resistance is through the end-user, not through sophisticated cyberattacks that target networks and systems. That's why people like you are referred to as "the last line of defense."

You are the final measure of security. You help identify phishing attacks, you ensure that the secured areas stay secure, and you protect your accounts with strong, unique passwords. Of course, new security technologies frequently land on the marketplace that help prevent security incidents. But if they were perfect, the words on this page wouldn't need to exist. Email filters and firewalls provide great examples: they block 99% of malicious messages and spam, but that 1% still exists. And it's up to you, the last line of defense, to be the human firewall.

The Impacts of Data Breaches

To get a clearer picture of a data breach's impacts, let's break it down into two categories:

Organizational Impacts

- Loss of revenue
- Violation of compliance regulations (leading to fines and legal action)
- Damaged reputation and destruction of public trust
- Expensive recuperation efforts

Individual Impacts

- Loss of confidential data such as residential address, national ID number, banking information
- Identity theft (where a criminal uses the stolen data to open fraudulent accounts)
- Damaged credit and financial loss
- Difficult, long-term recovery

These consequences are just a few examples of how data breaches impact everyone. As the last line of defense, you play a major role in our combined efforts to prevent breaches and ensure our organization protects the data entrusted to us.

Remember, when you have access to confidential information, you become responsible for that information. It's your job to prioritize security no matter your job title or level of access. As always, if you have questions, please ask.