SecurityAwarenessNews
the security awareness newsletter for security aware people

The Fundamentals of Data Protection

How Data Gets Leaked or Stolen
Protecting Confidential Information
The Internet's Hidden Layers

© 2026 KnowBe4, Inc. All rights reserved. | www.knowbe4.com

How Data Gets Leaked or Stolen

Understanding how data gets stolen or leaked is a crucial step in building a strong defense. Many data breaches fall into one of these three categories: cyberattacks, social engineering, and human error.

Cyberattacks

These are often technical attacks where criminal hackers sometimes use automated tools to bypass security defenses.

The How:

Attackers often probe networks for weaknesses that could provide access to data and systems.

The Goal:

Once inside, they can monitor communications and identify other weaknesses that may lead to large-scale attacks.

Example:

Criminal hackers could use a form of malware that encrypts and steals data. They then demand a large payment to unlock the data or to prevent it from being leaked.

Social Engineering

Rather than hacking devices, these attacks hack people. This is known as social engineering: the art of deceiving people through emotional manipulation.

The How:

The most common tactic is phishing, which uses misleading emails, texts, or calls that appear to be from a trusted source.

The Goal:

To trick people into opening dangerous links or attachments, or convince them to volunteer confidential information, such as passwords.

Example:

An urgent email that claims an account has been suspended due to fraudulent activity. It asks you to immediately confirm your password to prevent the account from being permanently locked.

Human Error

Sometimes, a data leak isn't the result of a malicious attack at all. Instead, it happens because of a simple mistake.

The How:

Mistakes often result from people moving too quickly, multitasking, or failing to follow organizational policies.

The Result:

In these cases, there is no initial attacker, but mistakes can still lead to leaks that allow data to fall into the attackers' possession.

Example:

Someone accidentally sends a confidential spreadsheet to the wrong recipient, or a developer leaves a database open to the public internet due to a misconfigured setting.

The Takeaway:

Protecting data requires slowing down, staying alert for red flags, and ensuring your software is always up to date.

© 2026 KnowBe4, Inc. All rights reserved. | www.knowbe4.com

Protecting Confidential Information

Data privacy and security require a layered approach to ensure confidential information remains confidential. Let's review a few ways you can help protect data, and by extension, people.

Learn the Warning Signs

Attackers will attempt to steal data through various methods, including phone calls, emails, and other forms of communication. Many of their efforts can be identified by staying alert for warning signs. Urgent requests, threatening language, and unexpected links or attachments are all indicators of scams to be aware of.

Avoid Assumptions

Remember, skepticism is your friend. The unfortunate reality is that modern technology allows cybercriminals to convincingly impersonate the people we know and trust. Avoid assuming that someone is who they claim to be or that any particular scenario or request is real. Take time to verify before revealing any confidential information.

Protect Your Access

Gaining access to accounts and networks is a primary objective of attackers. It is therefore vital to protect your access by using strong, unique passwords for every account and never sharing your passwords or other forms of access, such as ID badges, with anyone for any reason.

Implement Multi-Factor Authentication

Multi-factor authentication, or MFA, is a vital security tool for keeping accounts secure. It requires at least two forms of authentication before access to an account is granted. Implement MFA wherever it's available. For even stronger security, consider using a phishing-resistant MFA option, such as a USB stick or token. This is a much better process than having MFA codes delivered via text or email, which can be stolen.

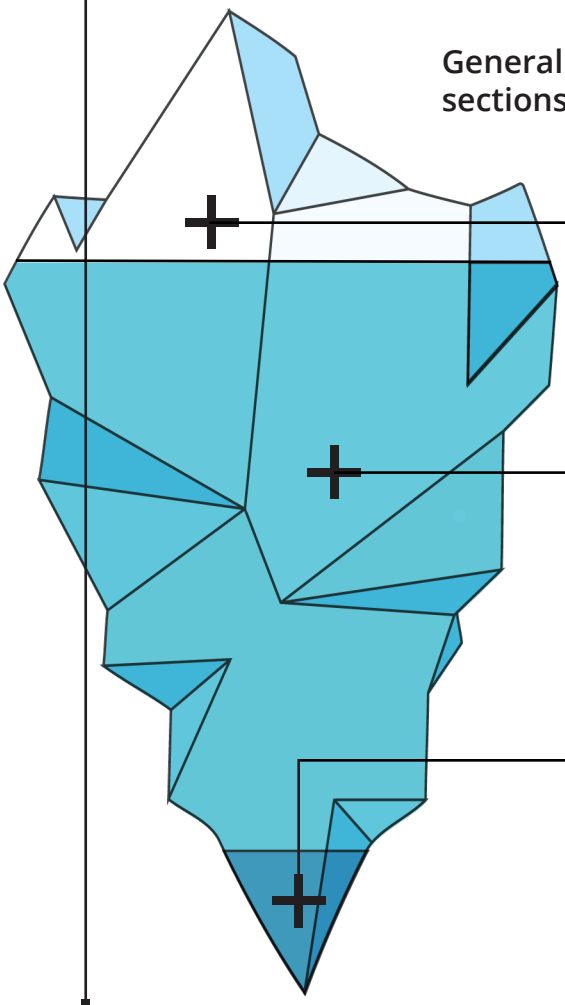
Follow Policy

Protecting data is sometimes as simple as following organizational policies. These are designed to minimize risk to data and people and prevent authorized access to confidential information. Failure to follow policy, whether intentionally or otherwise, could undermine everyone's security efforts.

© 2026 KnowBe4, Inc. All rights reserved. | www.knowbe4.com

The Internet's Hidden Layers

The World Wide Web includes perhaps billions of websites. But did you know that those sites only represent a tiny fraction of the Web? To protect your organization (and yourself!), it helps to understand what lies beneath the surface.



Generally, the World Wide Web is categorized into three sections: the Surface Web, the Deep Web, and the Dark Web.

The Surface Web

This is the public internet you use every day. It includes sites like Google, Amazon, news outlets, social media, and more. If you can find it via a search engine, it's on the Surface Web.

The Deep Web

Making up about 90% of the internet, this layer includes password-protected pages, such as your online banking and other accounts, medical records, and internal portals. It is hidden from search engines to keep your personal data safe.

The Dark Web

A tiny, hidden sliver of the Deep Web that requires special software to access. Because it offers total secrecy, it is a haven for both the good (such as providing a refuge for journalists at risk of political punishment or censorship) and the bad (cybercriminals).

A Journey Into the Dark Web

The Dark Web acts as an underground marketplace: When data is stolen through phishing scams and other attacks, it is often sold there. The key to avoiding this is protecting the access you've been granted. Here's how:

Use strong, unique passwords: If one site is breached and your password ends up on the Dark Web, attackers will try to use it on other sites, hoping to find a match. Never use the same password twice.

Stay alert: Data is often leaked or stolen when people make mistakes, like opening malicious links or attachments. Don't let this happen to you. Stay alert, slow down, and be especially careful when handling private information.

Keep confidential data off the Surface Web: Never put private information into public forums, tools, or unsecured file-sharing sites.

© 2026 KnowBe4, Inc. All rights reserved. | www.knowbe4.com