K2's Securing Your Data – Practical Tools For Protecting Information

Continuing Professional Education Series



K2 Enterprises www.k2e.com

K2E Canada Inc. www.k2e.ca

Copyright © 2026, by K2 Enterprises and K2E Canada Inc.

All rights reserved. No part of this publication may be reproduced or transmitted in any form without the express written consent of:

K2 Enterprises
1905 W. Thomas St., Suite D #363
Hammond, LA 70401-2901
985.542.9390

K2E Canada Inc.
174 Brewer Court
Burlington, Ontario, L7L4G4
905-746-1581

You may email requests to reproduce or transmit to info@k2e.com or caroline@k2e.ca. You may also obtain additional information on the web at www.k2e.com or www.k2e.ca.

The use of trade names and trademarks in these materials does not convey endorsement of these vendors or products. All trade names and trademarks used in these materials are the property of their respective owners. Any abbreviations used herein are solely for the reader's convenience and do not constitute any intent to compromise trademarks.

The statements in these materials about specific companies or specific hardware and software products should in no way be misconstrued as statements of fact but rather are opinions of the authors and K2 Enterprises and K2 Canada Inc. We take great care in providing views that we think will be useful in helping our participants make informed decisions. K2 Enterprises and K2 Canada Inc. reserve the right to independently evaluate companies' merits and the hardware and software products referenced in our seminars and conference presentations.

K2 Enterprises and K2 Canada Inc. make no representations or warranty regarding the contents of these materials and disclaim any implied warranties of merchantability or fitness for any particular purpose. The contents of these materials are subject to change without notice.

CONTRIBUTORS: The shareholders, associates, and staff of K2 Enterprises and K2 Canada Inc. contributed to producing these materials.

Introduction

Three Rules of this Seminar

1. **There Are No Dumb Questions.** Please ask questions if you need further explanation. We welcome your questions and will do our best to provide accurate and meaningful answers.

2. **Obtain the Information for Which You Came.** If you have a specific interest in a topic, please let us know. If your topic is not part of the course materials, we will do our best to accommodate your request. Your instructor is anxious to meet your needs.

3. **Share and Share-Alike.** Your instructor is here to share relevant information about the course. We hope that you will be willing to do the same. If you have helpful tips or experiences, please share them with the other participants and us.

Course Development

The shareholders, associates, and staff of K2 Enterprises and K2E Canada Inc. developed this course and the related course materials. We aim to deliver high-quality educational practices that help you use and understand the tools and concepts discussed in this session more effectively.

We designed our course presentation style for busy professionals. Through numerous short case studies and feature reviews, we deliver concise, easy-to-understand, easy-to-absorb information.

To maximize your time and the value of attending this course, we have carefully filtered out trivial and obscure features. Our goal is not to cover every keystroke and menu option, but to provide a fast-paced course that focuses on state-of-the-art information technology and how it can benefit you and your staff.

About K2 Enterprises

For over three decades, our team members have delivered more than 45,000 technology-focused seminars, webinars, and conferences worldwide. To stay on top of technology, our team members read numerous technology trade magazines, attend conferences, and speak with technology companies each year to stay current with the latest information for our courses. Also, we experience everything we teach and recommend to our audiences. Because our shareholders and associates are based in different states and provinces, using technology efficiently and appropriately is essential to our business's success and survival.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Our Mission Statement

K2 aims to develop and deliver the highest-quality technology seminars and conferences for business professionals. We work cooperatively with professional organizations such as state CPA societies, associations of Chartered Professional Accountants, and technology vendors. We make every effort to maintain high integrity, family values, and friendship among all involved.

Our Instructional Team

For a complete listing of instructors and bios, please visit:

K2 Enterprises

Instructors - K2 Enterprises

K2E Canada Inc.

Instructors - K2E Canada Inc

The K2 Seminar Curriculum

Full-day Seminars

- K2's Advanced Excel
- K2's Business Intelligence, Featuring Microsoft's Power BI Tools
- K2's Case Studies In Fraud And Technology Controls
- K2's Excel Best Practices
- K2's Excel Essentials For Staff Accountants
- K2's Excel PivotTables For Accountants
- K2's Excel Tips, Tricks, And Techniques For Accountants
- K2's Next Generation Excel Reporting
- K2's QuickBooks For Accountants
- K2's Small Business Internal Controls, Security, And Fraud Prevention And Detection
- K2's Technology For CPAs – Don't Get Left Behind

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Half-day Seminars

- K2's Artificial Intelligence For Accounting And Financial Professionals
- K2's Best Word, Outlook, And PowerPoint Features
- K2's Better Productivity Through Artificial Intelligence and Automation Tools
- K2's Case Studies In Fraud And Technology Controls
- K2's Data Analytics For Accountants And Auditors
- K2's Ethics And Technology
- K2's Excel Charting And Visualizations
- K2's Implementing Internal Controls In QuickBooks Online Environments
- K2's Improving Productivity With Microsoft 365Cloud Applications And Services
- K2's Mastering Advanced Excel Functions
- K2's Microsoft Teams
- K2's Securing Your Data: Practical Tools For Protecting Information
- K2's Technology Update
- K2's Top PDF Features You Should Know

Besides the seminars listed above, K2 also produces numerous one and two-day technology conferences annually. You can find a complete listing of our course offerings, including dates, locations, and course descriptions, on our website at:

K2 Enterprises
Technology Conference - K2 Enterprises

K2E Canada Inc.
Technology Conference - K2E Canada Inc.

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

On-Site Training

Working cooperatively with state CPA organizations and associations of Chartered Professional Accountants, we are pleased to offer all our seminars and conference sessions as on-site training opportunities. On-site training provides companies of all sizes with numerous advantages, including the following.

- ***Customization***. K2 can customize the content of all on-site training events to meet your organization's specific needs. For example, we can combine selected parts of existing courses into a focused learning experience to meet your team's needs. Likewise, we can develop custom content from the ground up and deliver it to your team members, ensuring we meet your training objectives.

- ***Cost savings***. For organizations of all sizes, on-site training can provide significant cost savings compared to public training venues. In addition to potentially reduced registration fees, these cost savings materialize in the form of reduced travel costs and reducing the amount of time team members spend away from the office.

- ***Convenience***. Because you select your on-site training event's date, time, and location, on-site training is more convenient for you and your team than traditional training options. Many organizations schedule on-site training with staff meetings, retreats, and customer/client events to leverage the value of all participants' time.

Customization, ***cost savings***, and ***convenience*** are the three C's of "training to go." For more information on how you and your organization can experience these benefits or schedule an on-site training event, please visit:

K2 Enterprises
On-site Training - K2 Enterprises

caroline@k2e.com

K2E Canada Inc.
Seminars - K2E Canada Inc

caroline@k2e.ca

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Web-Based Training

K2 offers web-based CPE and CPD to accounting and business professionals throughout the United States and Canada. K2's award-winning instructors deliver two-, four-, and eight-hour webinars on numerous technology-focused topics.

Additionally, K2 provides on-demand training. On-demand courses offer you the advantage of receiving top-quality training at a time and location that fits your busy schedule. You can start a class today and complete it in the future. For more information, please visit:

For more information on either platform, please visit:

K2 Enterprises
Webinars - K2 Enterprises

K2E Canada Inc.
Webinars - K2E Canada Inc

K2 Internet Sites

K2 maintains multiple websites containing information and links relevant to CPAs and other business professionals as a service to the profession. Further, the content of these sites can enrich your experience during and after our seminars. In addition, our pages contain links to some of the top accounting and content management software solutions and even to a few sites that are just fun places to visit. If you have any comments or questions regarding our web pages, please email *webmaster@k2e.com*.

K2 has two primary websites. You can view information regarding CPE and CPD opportunities, access a library of technology tips and articles, and link to K2-related websites.

www.k2e.com

www.k2e.ca

Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

www.cpafirmtech.com

CPA Firm Technology contains technology-related information explicitly targeted at public accounting firms. We include product reviews, hardware and operating system discussions, affinity programs for CPA firms, and Cloud computing resources.



www.accountingsoftwareworld.com

Accounting Software World provides information related to accounting and financial management solutions. Here, you can find software and service reviews, product comparisons, white papers, and other material of interest to those seeking information about accounting software and service solutions.



www.totallypaperless.com

For information about document management and paperless processes, please visit **Totally Paperless**. In addition, you will find reviews on hardware and software used by all types of businesses in document imaging and management processes.



Copyright © 2026. Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Learning Objectives



Assess the relevant security risks in your organization

Identify specific tools and techniques to protect sensitive data

List five specific steps to improve PC security

Implement security procedures to improve organizational security

Copyright 2026, K2 Enterprises, LLC



LET'S GET STARTED WITH SOME EXAMPLES OF HACKS AND ATTACKS

Copyright 2026, K2 Enterprises, LLC

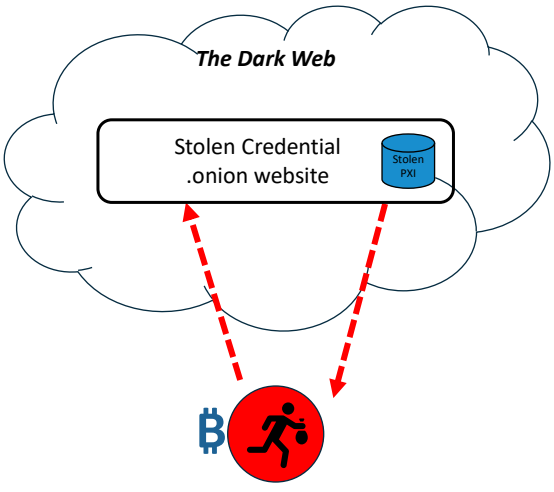
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Firm's Password "Manager" Hacked

- Passwords – considered a necessary evil by many – remain a critical component of many organizations' security practices
- In one recent data breach, a firm **stored passwords for critical systems in an unencrypted Excel file**
- As a result, hackers gained access to sensitive client data, including tax returns and Social Security numbers
- Unfortunately, this was only the beginning…
  - https://whizkids.tech/blog/cpa-firm-excel-data-breach/

Copyright 2026, K2 Enterprises, LLC

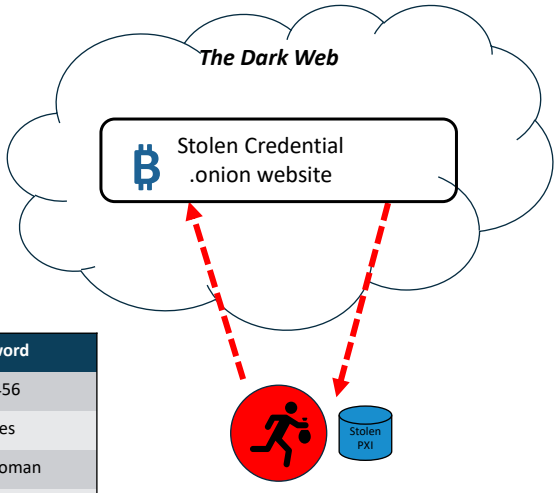
A Credential Stuffing Attack



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

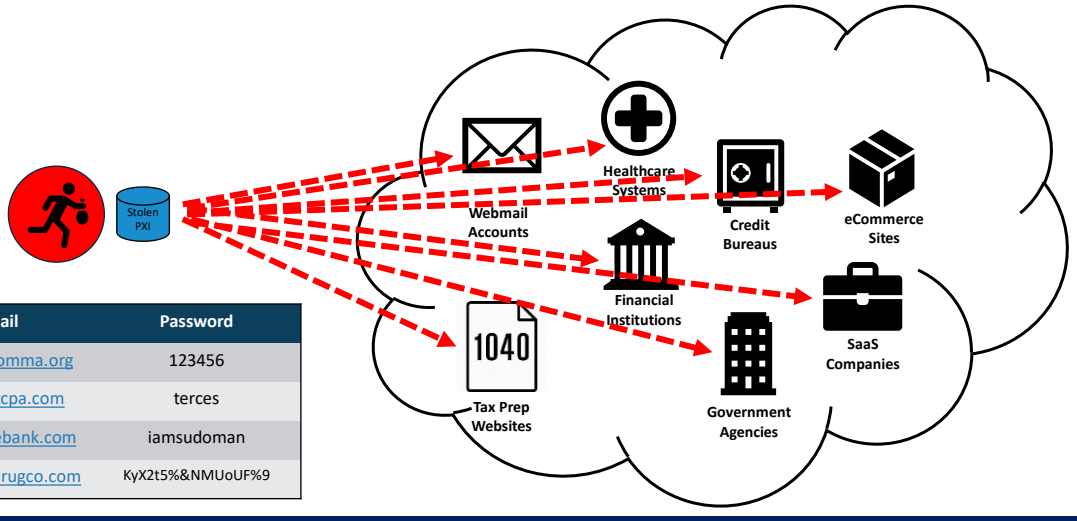
A Credential Stuffing Attack



E-mail	Password
joe@joemomma.org	123456
ralph@bftcpa.com	terces
admin@thebank.com	iamsudoman
paranoid@drugco.com	KyX2t5%&NMUoUF%9

Copyright 2026, K2 Enterprises, LLC

Anatomy Of A Credential Stuffing Attack



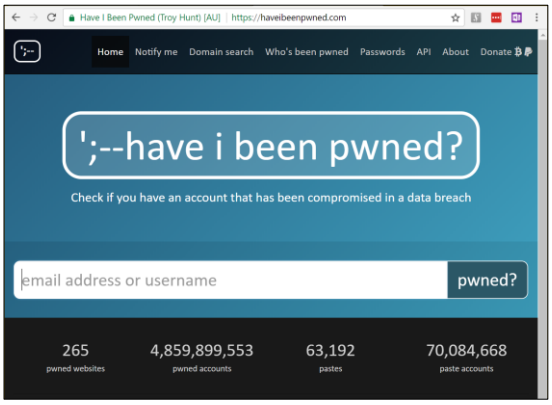
E-mail	Password
joe@joemomma.org	123456
ralph@bftcpa.com	terces
admin@thebank.com	iamsudoman
paranoid@drugco.com	KyX2t5%&NMUoUF%9

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Are Your Credentials At Risk?

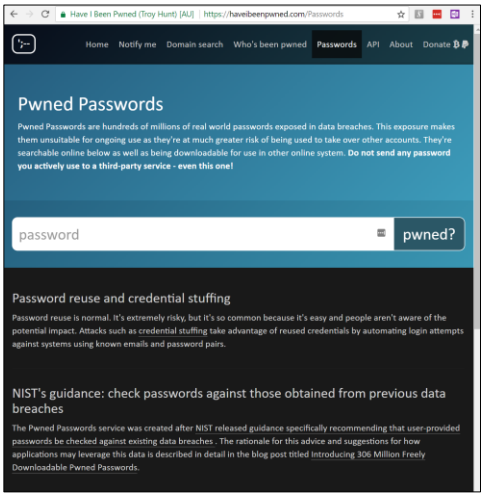
- Visit haveibeenpwned.com, run by security researcher Troy Hunt
- Enter your e-mail address or usernames and see which online data dumps have included them
- IT admins can also search for any users at an Internet domain (e.g. k2e.com) which has credentials compromised in a previous hack



Copyright 2026, K2 Enterprises, LLC

Are Your Credentials At Risk?

- Check your old passwords (which you should never reuse) against the online database at haveibeenpwned.com/Passwords
- Your IT department can also download the entire database of previously used passwords (converted to SHA1 hashes) so you can check user-provided passwords against data breaches



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Phishing Attack Leads To Breach

- According to the Journal of Accountancy (6/18/2025) a Texas-based CPA firm was attacked through a **phishing scheme** in 2022
- In this case, a part-time employee clicked on an email appearing to originate from Microsoft
  - The message instructed the staff member to "Click here to keep using your password" and also asked her to enter the password
  - Of course, the employee clicked and entered her password, which, of course, rendered other internal controls useless, including MFA, because the attackers had control of her email account

Copyright 2026, K2 Enterprises, LLC

CPA Firm Has 217k Records Breach

- As reported in the HIPAA Journal, Legacy Professionals (an Illinois CPA firm) experienced a breach of 217,000 records
- Compromised information included employee benefit plan info – names, SSNs, driver's license numbers, medical treatment information, health insurance information, etc.
  - The data was published to the Dark Web
- The Firm is being sued for negligence for failing to implement reasonable safeguards and for not reporting the incident until 10 months after the breach occurred

Copyright 2026, K2 Enterprises, LLC

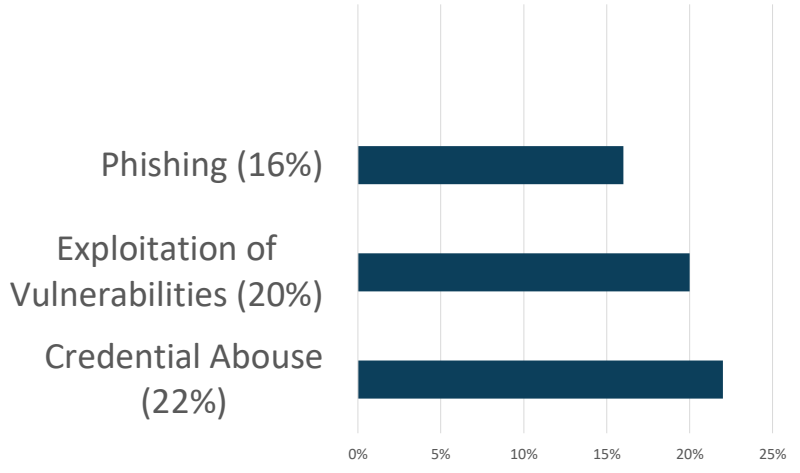
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Think about these at a corporate level and at a personal level

WHERE ARE YOUR BIGGEST RISKS? KEY FINDINGS FROM VERIZON'S 2025 DATA BREACH INVESTIGATIONS REPORT

Copyright 2026, K2 Enterprises, LLC

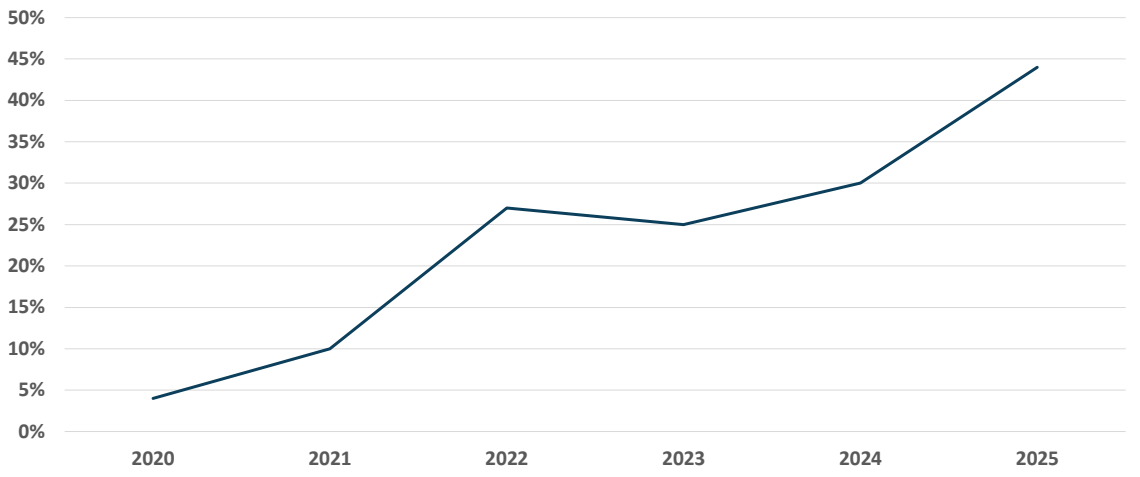
What Vulnerabilities Get Exploited



Copyright 2026, K2 Enterprises, LLC

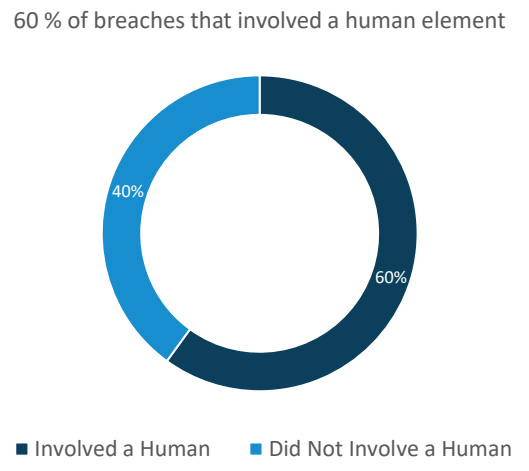
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Ransomware Continues To Grow



Copyright 2026, K2 Enterprises, LLC

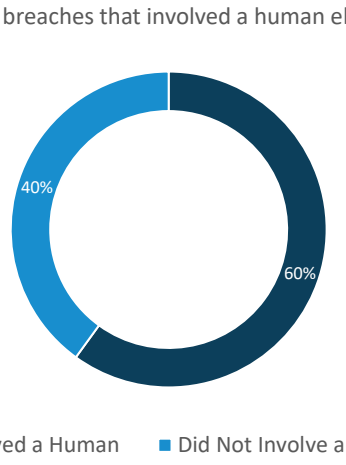
Sorry, But We As Humans Are A Big Part Of The Problem



Copyright 2026, K2 Enterprises, LLC

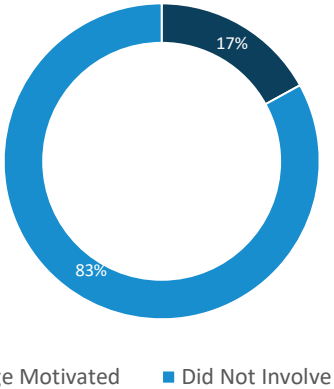
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Third Parties Are Involved In 30% Of All Breaches (including software vulnerabilities)



Copyright 2026, K2 Enterprises, LLC

Espionage Motivated 17% Of Breaches



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

GenAI Can Introduce More Risk



- A large number of AI users (72%) are logging in with their individual accounts, not corporate accounts
- This potentially allows bad actors to intercept and exploit data that is likely being used outside of corporate policy

Copyright 2026, K2 Enterprises, LLC



SUMMARY BY INDUSTRY

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Educational Services
(NAICS 61)

Frequency	1,075 incidents, 851 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 80% of breaches
Threat actors	External (62%), Internal (38%) (breaches)
Actor motives	Financial (88%), Espionage (18%) (breaches)
Data compromised	Personal (58%), Internal (49%), Other (35%), Credentials (12%) (breaches)
What is the same?	System Intrusion, Miscellaneous Errors and Social Engineering are still the top three patterns, as they have been for the last two years.
Summary	While we saw a decrease in the number of both incidents and breaches in the Educational Services industry, the attacks that we did see were along the lines of what we have seen in the past. System Intrusion is far and away the top pattern, and it is driven by financially motivated External actors.

Copyright 2026, K2 Enterprises, LLC

Financial and Insurance
(NAICS 52)

Frequency	3,336 incidents, 927 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 74% of breaches
Threat actors	External (78%), Internal (22%), Partner (1%) (breaches)
Actor motives	Financial (90%), Espionage (12%) (breaches)
Data compromised	Personal (54%), Other (44%), Internal (35%), Credentials (22%) (breaches)
What is the same?	System Intrusion remains the top pattern once again, due to the preponderance of more complex attacks. Dare we hope this is because the adversaries are having to expend more effort?
Summary	The Financial and Insurance vertical is still dominated by financially motivated threat actors who will usually take any data type they can lay their hands on. However, attacks with the motive of Espionage have increased this year.

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Healthcare
(NAICS 62)

Frequency	1,710 incidents, 1,542 with confirmed data disclosure
Top patterns	System Intrusion, Everything Else and Miscellaneous Errors represent 74% of breaches
Threat actors	External (67%), Internal (30%), Partner (4%), Multiple (1%) (breaches)
Actor motives	Financial (90%), Espionage (16%) (breaches)
Data compromised	Medical (45%), Personal (40%), Internal (32%), Other (24%) (breaches)
What is the same?	The attack patterns remain the same, although they have changed position since last year.
Summary	The Healthcare sector remains a prime target for cyberattacks and shows a slight increase in incidents and breaches this year. System Intrusion (including Ransomware) has overtaken Miscellaneous Errors as the top cause of breaches. The rise of Espionage as a motive for attackers in this sector is concerning.

Copyright 2026, K2 Enterprises, LLC

Manufacturing
(NAICS 31-33)

Frequency	3,837 incidents, 1,607 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (86%), Internal (14%) (breaches)
Actor motives	Financial (87%), Espionage (20%) (breaches)
Data compromised	Internal (64%), Other (37%), Personal (33%), Credentials (22%) (breaches)
What is the same?	System Intrusion, Social Engineering and Basic Web Application Attacks are still the top three patterns, with the majority of attacks continuing to come from financially motivated External actors.
Summary	This year, 1 in 5 breaches were due to Espionage-motivated actors as compared to last year's 3%. Internal (sensitive plans, reports, email) is, by far, the most commonly stolen data type. And more than 90% of breached organizations were SMBs with fewer than 1,000 employees.

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Retail
(NAICS 44-45)

Frequency	837 incidents, 419 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 93% of breaches
Threat actors	External (96%), Internal (3%), Partner (1%) (breaches)
Actor motives	Financial (100%), Espionage (9%) (breaches)
Data compromised	Internal (65%), Other (30%), Credentials (26%), Payment (12%) (breaches)
What is the same?	The top three patterns in this industry have not changed from last year—neither their membership nor their order.
Summary	The Retail industry has seen an increase in cyber incidents, though the focus has shifted from Payment card data to other data types that are easier to access. There was a notable rise in Espionage-motivated attacks as compared to last year. Defenders should be aware of more sophisticated and harder-to-detect threats.

Copyright 2026, K2 Enterprises, LLC

Public Sector
(NAICS 92)

Frequency	1,422 incidents, 946 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 78% of breaches
Threat actors	External (67%), Internal (33%), Partner (1%) (breaches)
Actor motives	Financial (76%), Espionage (29%), Ideology (2%) (breaches)
Data compromised	Personal (47%), Internal (44%), Other (41%), Secrets (17%) (breaches)
What is the same?	This industry continues to be plagued by sophisticated attackers looking to gain access to the trove of data collected by governments about their constituents. Though the majority of breaches were from External actors, a significant number were from Internal actors making simple mistakes.
Summary	While we show a drop in reported incidents due to the makeup of contributors this year, the number of confirmed breaches remained steady. This means attackers are not easing up on government targets. Ransomware remains a major threat, hitting 30% of breaches across all levels of government. Errors remain a persistent issue, with Misdelivery in the lead.

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Focusing On North America

Northern America (NA)



Frequency	6,361 incidents, 2,867 with confirmed data disclosure
Top patterns	System Intrusion, Everything Else and Social Engineering represent 90% of breaches
Threat actors	External (91%), Internal (5%), Partner (5%), Multiple (1%) (breaches)
Actor motives	Financial (95%), Espionage (9%) (breaches)
Data compromised	Internal (49%), Medical (35%), Credentials (23%), Other (17%) (breaches)

Copyright 2026, K2 Enterprises, LLC

WHAT DO WE TAKE AWAY FROM THESE STATISTICS?

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Key Takeaways From The Numbers



- Every individual and every organization is at risk!
- Your risks vary based on the type of business you are in and on other critical factors including technology and training
- Yes, the Internet creates opportunities for data breaches, espionage, etc., but were you able to secure paper?

Copyright 2026, K2 Enterprises, LLC

Today's Common Critical Risks



- Ransomware
- Social engineering
- Unencrypted data
- Poor authentication controls
- Poor patch management on computing devices
- Exposure through trading partners
- BYOD and IoT

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What's The Fallout?



- Down time and lost productivity
- Security breaches and compromises of confidential information, particularly where there is fiduciary responsibility
- Reputation loss, but that's not as much as it used to be, because virtually everyone and every organization in the US has already been compromised

Copyright 2026, K2 Enterprises, LLC

The Major Attack Vectors



- Email
  - Attached files
  - Links
- Web sites
- Direct attacks to the cloud, to your premise-based system, your computers, or your mobile devices
- Fraud committed by employees or external providers

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Is Your Information Compromised? Probably!

- By the time your information hits the dark web, it is WAY too late for you to do anything
- Terbium Labs – Matchlight – five searches for free
- SpyCloud – One of our favorites
- ';--have i been pwned? https://haveibeenpwned.com/
- Also, a free check from www.experian.com (ironic isn't it?)
- Additionally, all business credit cards should be set up for automatic alerting, particularly for foreign transactions

Copyright 2026, K2 Enterprises, LLC

The Most Important Consideration…

- Humans are the weak link in the security chain!
  - Data breaches and security failures are almost always human-caused, not technology caused
- We must do a better job of training our team members
- A great place to start is by training to effective policies
  - See the resources available at **The SANS Institute's Security Policy Project** (www.sans.org), a free resource for all
- Remember, most of your team members **want** to do the right thing…they just need to know what that is!

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Let's Understand It So That We Can Defend Against It

WHAT IS RANSOMWARE?

Copyright 2026, K2 Enterprises, LLC

What Is Ransomware?

Ransomware is a form of malware that targets your critical data and systems for the purpose of extortion. Ransomware is frequently delivered through spearphishing emails. After the user has been locked out of the data or system, the cyber actor demands a ransom payment. After receiving payment, the cyber actor will purportedly provide an avenue to the victim to regain access to the system or data. Recent iterations target enterprise end users, making awareness and training a critical preventive measure.[1]

[1] *"How to Protect Your Networks from Ransomware"*

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Is Ransomware?



- Ransomware is yet another form of malware, similar in some regards to viruses, worms, Trojan Horses, and the like
- When ransomware strikes, it typically takes control of the data files on a computer and holds them "hostage" until the victim pays a ransom demanded by the cybercriminals
  - If the victim pays the ransom, the cybercriminals (in theory) return control of the data files held hostage to the victim
  - If the victim does not pay the ransom, then access to the files is lost forever

Copyright 2026, K2 Enterprises, LLC

How Does Ransomware Take Control Of Files?



- Generally, one of two techniques are used to take control of the data files on a computer infected by ransomware
  1. The files are encrypted with a strong password, and the cybercriminals do not provide the password to the victim until the ransom is paid
  2. The cybercriminals copy the files from the victim's computer and then delete them from the victim's computer after copying; upon receipt of the ransom payment, the cybercriminal copies the files back to the victim's computer//not as common as it once was
- Regardless of the scenario, if you are the victim, <u>you will be unable to access your data without paying the ransom, and possibly (perhaps likely) even if you do pay the ransom</u>

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

You Be Your Own Judge!

SHOULD YOU REALLY BE CONCERNED?

Copyright 2026, K2 Enterprises, LLC

If You Become Infected With Ransomware, It May Look Like This



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

EXAMPLES OF HIGH-PROFILE ATTACKS

Copyright 2026, K2 Enterprises, LLC

High-Profile Ransomware Attacks

City of New Orleans

- Came on the heels of a similar attack on the State of Louisiana government
- **Affected over 4,000 computers** owned by the city's government
- **$7 million in damages, with $3 million recovered through cyber insurance** policy//in the aftermath, the city increased its coverage to $10 million
- Believed to have been caused by **Ryuk** and perpetrated by organized crime
- In addition to financial costs, resulted in the City government declaring a State of Emergency in the city

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

High-Profile Ransomware Attacks

City of Atlanta

- Hackers used **SamSam** to cripple city government, including court scheduling, online bill payments, airport Wi-Fi, copies of emails being destroyed, dashboard-mounted camera video from police being lost, etc.
- Ransom demand was $52,000… ultimately, **city paid upwards of $17 million in remediation costs**
- January 2018 **audit exposed approximately 2,000 vulnerabilities** in city's Information Technology infrastructure
- Two people were arrested in November 2018…they were believed to have been behind **200 attacks**, netting more than **$6 million in ransom**, including attacks involving **Newark**, **Port of San Diego**, and **Colorado Department of Transportation**

Copyright 2026, K2 Enterprises, LLC

High-Profile Ransomware Attacks

- Colonial Pipeline provides a **MAJOR** pipeline that transmits gasoline, diesel fuel, and aviation fuel throughout the Southeast and up the mid-Atlantic regions of the US
- Ransomware struck on May 7, 2021 crippling the company's software that managed the pipeline
- Hackers were able to penetrate Colonial's systems because of weak authentication controls
- Reports indicate that Colonial paid the ransom, but ultimately recovered from backups

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Some Trends Have Emerged

- Formerly targeting individuals almost exclusively, ransomware is an increasing threat to businesses, governments, health care providers, schools….**EVERY PERSON** and **EVERY ORGANIZATION!**
- According to PURPLESEC (https://purplesec.us/learn)
  - The average cost of an attack is $5.13 million
  - That cost has increased 574% over the past 6 years
- According to Ponemon Institute, 51% of businesses choose to pay the ransom
  - However, doing so could violate US law

Copyright 2026, K2 Enterprises, LLC

GIVEN THE NUMBERS, CAN YOU AFFORD TO IGNORE THE RISKS?

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Are Your Risks?

- If you are infected with ransomware, absent a good backup, you very well may lose access to all your data files!
  - This could, of course, result in a substantial disruption of your business, potentially causing loss of customers/clients and reputation in the market
  - It also could cause you to lose important personal data files, such as pictures, videos, and PDF documents
- Additionally, ransomware may constitute a reportable incident under state/provincial security breach notification laws and/or HIPAA

Copyright 2026, K2 Enterprises, LLC

Ransomware As Potential HIPPA Violations

According to Health and Human Services:

A breach is, generally, an impermissible use or disclosure under the privacy rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Ransomware As Potential HIPPA Violation

1. *The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;*
2. *The unauthorized person who used the protected health information or to whom the disclosure was made;*
3. *Whether the protected health information was actually acquired or viewed; and*
4. *The extent to which the risk to the protected health information has been mitigated.*

Copyright 2026, K2 Enterprises, LLC

Consider Ransomware Impacting A CPA Firm

- Suppose ransomware strikes a CPA firm the week before a tax filing deadline
- What are the firm's options?
  - Restore data from backup and continue operating, or
  - Pay the ransom and *HOPE* to continue operating, or
  - Tell clients that the firm won't be able to complete their individual income tax returns by the statutory due dates, that they can't compute how much should be paid with their extension request, and that they can't tell them how much their first quarter estimated tax payment should be

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

HOW RANSOMWARE ATTACKS YOU

Copyright 2026, K2 Enterprises, LLC

How Ransomware Attacks You

- There is no single source for ransomware…it can infiltrate and infect a computer or network using many different points of attack
- The nine most common methods today include
  1. ***Unsolicited email***, with malicious links or attachments…some refer to this as "malspam"
  2. ***Malicious URLs*** transmitted through social media
  3. ***Drive-by websites***, which are sites that are created specifically to distribute malware or legitimate sites that have been compromised to do the same
  4. Through ***open Remote Desktop Protocol (RDP) ports***
  5. ***Attacking Managed Service Providers*** to get to their customers

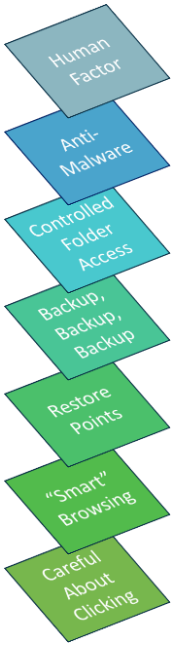
Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How Ransomware Attacks You

- The more common methods today include
  6. ***Lateral attacks***, spreading through an organization
  7. Embedded into ***free and pirated software***
  8. ***USB drives*** used to spread ransomware onto unsuspecting victims' computers and networks
  9. ***"Malvertising"*** on web pages

Copyright 2026, K2 Enterprises, LLC



One, Two, Or Three Steps Is Probably Not Adequate

PROTECTING YOUR DATA AND OTHER ASSETS FROM RISK REQUIRES A MULTI-LAYERED APPROACH

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Focus On Your Team!



Remember, we are only human and therefore, we are the weak link in the security chain

- Therefore, educate yourself and your team members on the risks associated with ransomware specifically and malware in general
- Include education and testing around clicking on attachments and links in unsolicited email messages
- Also, educate team members on the dangers associated with certain types of websites

Copyright 2026, K2 Enterprises, LLC

Activate Windows' Controlled Folder Access Feature



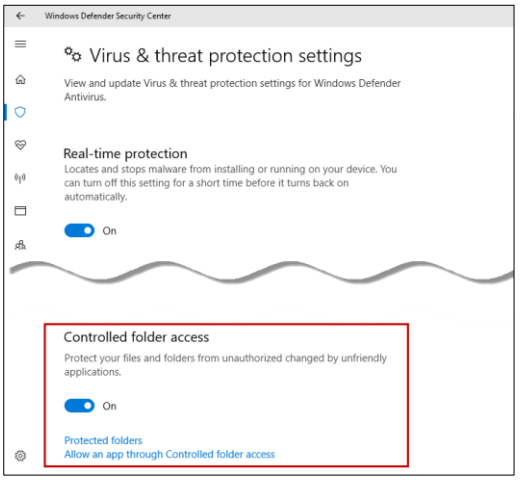
- Became available with Fall 2017 Creator's Update (version 1709)…in other words, it's not new!
- Enabled by users with Administrative privileges through the **Windows Defender Security Center**
  - Admins can enable through PowerShell and Group Policy, in addition to mobile device management configurations
- Once enabled, CFA prevents files in specific folders from being tampered with by unknown and potentially risky applications
- Essentially, CFA is a form of "whitelisting"

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Activate Windows' Controlled Folder Access Feature

- In Search Box, type **Windows Defender Security Center**
- In Navigation Bar, choose ***Virus & threat protection***
- Click **Virus & threat protection settings**
- Toggle "on" **Controlled folder access**
- Fine-tune by adjusting folders and apps



Copyright 2026, K2 Enterprises, LLC

Face What May Be Inevitable

- **Backup**, **Backup**, **Backup**!!! Ensure that you have a sound backup strategy in place and test it periodically to verify that you can recover 100% of your data
  - This is a fundamental tenet of computer and information security and extends above and beyond just addressing the risk of ransomware
  - Make sure that backup drives do not remain connected to individual computers or networks
    - Ransomware can "jump the fence" and get to your Cloud resources such as OneDrive
- Conduct periodic penetration testing and vulnerability assessments, including "white hat" attacks

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

If You Become A Victim



- Immediately isolate the infected computer(s) so that others on the network do not become affected
- Shut down devices that have not yet been completely corrupted
- Change all online account passwords and network passwords after removing the affected computer from the network
  - Also change all system passwords once the ransomware is eradicated
- Delete necessary Registry values to stop the program from loading

Copyright 2026, K2 Enterprises, LLC

If You Become A Victim



- Verify accessibility and integrity of backups
- Consider implementing your Incident Response plan and/or your Business Continuity plan
- Contact law enforcement immediately, namely a local field office of the FBI, US Secret Service, or RCMP

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

If You Become A Victim



- Should you pay the ransom?
  - It's a legitimate question…after all, in the absence of a backup, this may be your only way to recover your data
- However, first consider the following
  - Paying encourages the criminals to continue their activities
  - Paying ransom does not guarantee recovering your data
  - Those who pay the ransom are often targets for additional attacks
  - Sometimes the criminals attempt to extort more than the "advertised" amount of the ransom

Copyright 2026, K2 Enterprises, LLC

Summarizing Ransomware



- Ransomware is a real and substantial threat to everyone who uses a device connected to the Internet
  - Not just computers, but now even our mobile devices are targets
- If you are infected, there is a substantial chance that you will lose access to all your critical data
- A multi-layered approach to security – starting with proper education – can help to greatly reduce the risk that you will become a victim
- However, risk will remain so ensure that you have appropriate backups in place so that you can recover your data

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

THE IMPORTANCE OF LONG-AND-STRONG PASSWORDS

Copyright 2026, K2 Enterprises, LLC

Authentication Controls Are One Of Your First Lines Of Defense

- Passwords are meant to provide a form of *authentication* control
- They help to guard against unauthorized ***use*** of computers, tablets, smartphones, and other devices
- More importantly, they help to protect the ***data*** on these devices and also guard against unauthorized access to data stored on servers to which devices are connected

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How Hackers Compromise Passwords



- Guessing
- Dictionary attacks
- Brute force attacks
- Password sniffing software
- Social engineering

Copyright 2026, K2 Enterprises, LLC

		Assuming 5,000,000 Hack Attempts Per Second	
Password Length in Characters	Potential Universe of Passwords	Average Days to Hack	Average Years to Hack
1	95	0	0
2	9,025	0	0
3	857,375	0	0
4	81,450,625	0	0
5	7,737,809,375	0	0
6	735,091,890,625	1	0
7	69,833,729,609,375	81	0
8	6,634,204,312,890,620	7,678	11
9	630,249,409,724,609,000	729,455	999
10	59,873,693,923,837,900,000	69,298,257	94,929
11	5,688,000,922,764,600,000,000	6,583,334,401	9,018,266
12	540,360,087,662,637,000,000,000	625,416,768,128	856,735,299
13	51,334,208,327,950,500,000,000,000	59,414,592,972,165	81,389,853,387
14	4,876,749,791,155,300,000,000,000,000	5,644,386,332,355,670	7,732,036,071,720
15	463,291,230,159,753,000,000,000,000,000	536,216,701,573,789,000	734,543,426,813,409

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

		Assuming 5,000,000 Hack Attempts Per Second	
Password Length in Characters	Potential Universe of Passwords	Average Days to Hack	Average Years to Hack
1	95	0	0
2	9,025	0	0
3	857,375	0	0
4	81,450,625	0	0
5	7,737,809,375	0	0
6	735,091,890,625	0	0
7	69,833,729,609,375	3	11
9	630,249,409,724,609,000	729,455	999
10	59,873,693,923,837,900,000	69,298,257	94,929
11	5,688,000,922,764,600,000,000	6,583,334,401	9,018,266
12	540,360,087,662,637,000,000,000	625,416,768,128	856,735,299
13	51,334,208,327,950,500,000,000,000	59,414,592,972,165	81,389,853,387
14	4,876,749,791,155,300,000,000,000,000	5,644,386,332,355,670	7,732,036,071,720
15	463,291,230,159,753,000,000,000,000,000	536,216,701,573,789,000	734,543,426,813,409

If your password isn't sufficiently long, are you really protected?

Copyright 2026, K2 Enterprises, LLC

KEY CHARACTERISTICS OF EFFECTIVE, LONG-AND-STRONG PASSWORDS

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

According To The SANS Institute (www.sans.org)...



"Long-and-strong" passwords possess the following four characteristics:

1. Contain at least 12 alphanumeric characters
2. Contain both upper and lower case letters
3. Contain at least one number (0-9)
4. Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/)

Copyright 2026, K2 Enterprises, LLC

Other Suggestions From SANS



- Do not use the same password for business accounts and for personal accounts
- All system-level passwords should be changed at least quarterly
- All user-level passwords should be changed at least every four months
- Passwords must not be shared with anyone
- Never reveal passwords over the phone
- Do not use the "Remember Password" feature in apps or browsers
- In case of a suspected breach, change all passwords immediately

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



HOW PASSWORD MANAGEMENT TOOLS HELP

Copyright 2026, K2 Enterprises, LLC

Can We Really Do This?



- Is it realistic to expect that all team members can and will comply with the guidelines indicated previously?
  - **OF COURSE NOT!!!!**
- Sorry, but as humans, we are the weakest link in the security chain
- Thinking that all users can and will comply with the password policy guidelines is likely a recipe for a security breach

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

What Password Management Tools Do



- Password management tools help to automate the processes associated with creating, using, and managing your ever-growing list of passwords
- In general, if you can remember the password that you use to access your password management tool, it allows you to access and use all of the passwords that you store inside the tool
- Encryption, synchronization, secure sharing, breach notification, auditing, policy creation and enforcement – these are all some of the benefits and uses of password management tools

Copyright 2026, K2 Enterprises, LLC

Top Password Management Tools



- There are many great password management tools available today
- Most are so good that it is difficult to make a poor choice
- Nonetheless, we recommend checking out the review at PC Magazine's article at http://bit.ly/1cHINTA
- We will discuss four solutions that are representative of what is available in the market today

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Key Question Regarding Password Management Tools



- Individual or corporate use?
- Allow synchronization across multiple devices?
- Support for additional functions, such as filling forms?
- Import data into the solution/export out of the solution?
- Capture passwords automatically?
- Analyze your password and provide alerts on potentially weak ones?
- Support for multi-factor authentication?

Copyright 2026, K2 Enterprises, LLC



SUMMARIES OF SOME OF THE LEADING PASSWORD MANAGEMENT TOOLS AVAILABLE TODAY

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Examples Of Password Management Tools



RoboForm	https://www.roboform.com
Zoho Vault	https://www.zoho.com/vault/
Dashlane	https://www.dashlane.com
LastPass	https://www.lastpass.com/business/home

Copyright 2026, K2 Enterprises, LLC

RoboForm



- One of the early entrants into the market, RoboForm provides solutions for both individuals and businesses
- For individuals, RoboForm is available at no charge…for businesses, RoboForm for Business is priced as follows:
  - 1 to 10 users: $29.95 per year, per user
  - 11 to 25 users: $26.95 per year, per user
  - 26 to 100 users: $25.95 per year, per user
  - 101 to 1,000 users: $21.95 per year, per user
  - Over 1,000 users: Contact RoboForm for annual site license fee

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

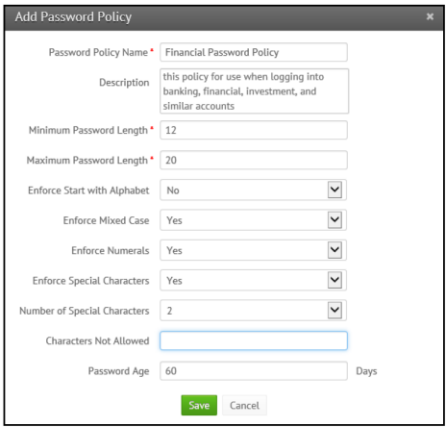
Zoho Vault

- Zoho bills itself as “the operating system for business” and offers 36 Cloud-based applications, including accounting, CRM, invoicing, payments, mail, and spreadsheets
- One of the apps in Zoho’s portfolio is **Vault**, a very good password management tool
- Vault is available in four versions
  1. Personal, free
  2. Standard (for small teams), $1 per user, per month
  3. Professional (minimum of five users), $4 per user, per month
  4. Enterprise (large teams, minimum of five users), $7 per user, per month

Copyright 2026, K2 Enterprises, LLC

Zoho Vault

- Vault provides exceptional functionality at modest pricing
- One key feature is the ability to create and enforce password policies across a workgroup
- With a policy, you can establish the mandated complexity of passwords for specific sites and applications or groups of sites and applications



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Additional Features In Zoho Vault For Corporate Users



- Securely sharing corporate passwords with team members
- One-time sharing of passwords with third-parties
- Password expiration alerts
- User groups
- User access and activity reports
- Notification of password-related event

Copyright 2026, K2 Enterprises, LLC

Dashlane



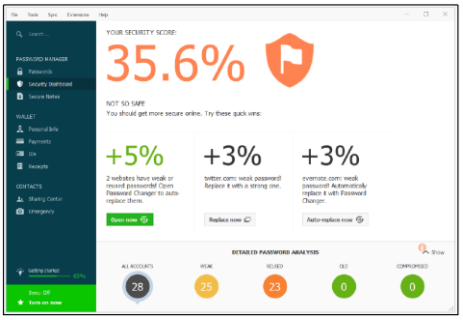
- **Dashlane** is a **PC Magazine's Editor's Choice**
- Three versions are available in the Dashlane portfolio
  1. **Dashlane Free**, no charge version to provide fundamental password management tools to individuals
  2. **Dashlane Premium** goes beyond functionality and provides synchronization across multiple devices and backing up password data for $39.99 per year
  3. **Dashlane Business** provides corporate-level management for businesses of all sizes, including organizations with greater than 1,000 employees. Pricing is $2 per user, per month for up to 100 users, $1.50 per user, per month
     for 101 to 1,000 employees, and $1.25 per user, per month for over 1,000 users

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Key Differentiating Features For Dashlane

- Dashlane can notify users of potential breaches
- For businesses, Dashlane allows a user to change a password used by multiple users
- Dashlane also “audits” your passwords and notifies you of potentially weak ones



Copyright 2026, K2 Enterprises, LLC

LastPass

- **LastPass** is also a well-respected tool, earning a **PC Magazine Editor’s Choice** award
- Like other tools, LastPass is available in multiple versions
  1. **LastPass** is a free tool that allows users to create, manage, and use passwords across all devices
  2. **LastPass Premium** is available for $1 per user, per month and adds fingerprint recognition and offers a “family” folder that can be shared by up to five users. Premium also supports logging into applications
  3. **LastPass Teams** (for fewer than 50 users) provides shared folders and user management for $2.50 per user, per month and Enterprise supports larger organizations for $4 per user, per month

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

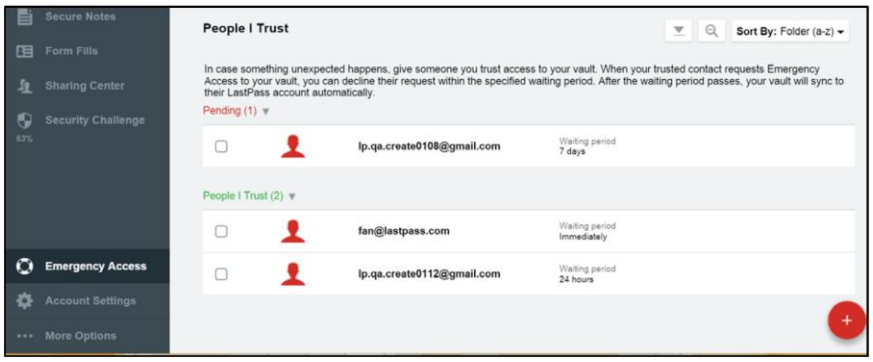
LastPass And Automatic Passwords

- LastPass integrates with over 80 websites and includes tools to create passwords automatically at these sites
- It also helps to identify weak or duplicated passwords

Copyright 2026, K2 Enterprises, LLC

LastPass And Emergency Access

- There is also an Emergency Access feature in case a user becomes incapacitated



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Why Consider Alternative Measures?



- Let's face it, even with password management tools, passwords are still a pain to create, manage, and update
- Further, as computers become ever more powerful, passwords will need to continue to get "longer-and-stronger" to remain useful
- However, with many alternative measures – retina scans and fingerprints, for example – there is no opportunity to change
- Thus, long-term use is facilitated, and security is enhanced

Copyright 2026, K2 Enterprises, LLC

Two Examples…



- **Windows Hello**
  - Feature in Windows 10/11 that allows users of compatible computers to log in using facial recognition
  - If Windows Hello doesn't recognize your face when it matches to your picture, you then log in with your password, PIN code, fingerprint, or picture password
- **Fingerprint Recognition**
  - Also embedded in Windows 10/11, you can log in using fingerprint recognition
  - Fingerprint recognition doesn't require Windows 10/11; you can simply purchase a keyboard with a fingerprint reader on it and most smartphones support it
  - Also, you can often use fingerprint recognition in tandem with your password management tools

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Multi-Factor Authentication



- **Multi-factor authentication (MFA)** typically involves something you know in addition to something that you have in your possession
  - For example, your password, plus a four or six-digit one-time use code sent to your smartphone or a key fob
- MFA means that someone attempting to break in to one of your accounts would need to know your user ID and password and have your smartphone or key fob in their possession to intercept the one-time use code and enter it
- An increasing number of applications support, including Microsoft 365, Google Workspace, QuickBooks Online, and many other Cloud-based tools…in fact, many now mandate its use

Copyright 2026, K2 Enterprises, LLC

Password Management Summary



- Passwords are, and will continue to be, and important element of our internal control structure to protect our sensitive data
- However, because of human error, the effectiveness of passwords for many individuals – and their organizations, by extension – is questionable at best
  - It is virtually impossible for individuals to comply with the guidelines for "long-and-strong" passwords
- Therefore, password management tools have emerged as an effective option for creating and managing passwords
- Looking forward, moving to alternative authentication measures makes a lot of sense as we try to strengthen our control structure

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



WHAT IS DATA LOSS PREVENTION AND HOW DOES IT ENHANCE ORGANIZATIONAL SECURITY?

Copyright 2026, K2 Enterprises, LLC

What Is Data Loss Prevention?



- Data Loss Prevention (DLP) tools are means of creating and enforcing security policies in an organization to reduce the risk of disclosing sensitive data, either accidentally or maliciously
- You can apply DLP tools at the network level, the endpoint level, or both
- When applied to the network, DLP tools analyze network traffic to detect potentially sensitive data
- When applied to endpoints, DLP tools can control data before it hits the network

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Why Is DLP Necessary?



- Let's use email as the example…we all know that email is a notoriously unsecure means of transmitting data, right?
- Yet according to a report in PC Magazine
  - 56% have sent email to the wrong person
  - 53% have received unencrypted emails containing sensitive info
  - 21% have sent sensitive corporate info without encryption
  - 20% know of someone at their company who has been caught sending sensitive info without following established security protocol

Copyright 2026, K2 Enterprises, LLC

Why Is DLP Necessary?



- But email isn't the only villain…consider the ubiquitous Excel spreadsheet stored on a shared drive on a corporate server
- Perhaps that workbook contains sensitive employee information, including Social Security numbers
- Why should everyone who has access to that drive be able to see the Social Security numbers for each employee whose name is recorded in the spreadsheet?
- Don't think this can happen? Consider what happened at WellPoint, Inc. where 128k customer records were potentially exposed while stored on an unsecured server

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

How Does DLP Enhance Security?



- In general, DLP tools analyze data in real-time, looking for patterns in the data that match certain specified characteristics
  - Social Security numbers and credit card numbers are good examples
- When a DLP tool finds data that appears to match a specific set of characteristics, it then takes the appropriate action as designated in the implementation
  - Perhaps simply sending a notification to the user and/or IT staff
  - Maybe blocking the traffic altogether, with or without notifications to the user and/or the IT staff

Copyright 2026, K2 Enterprises, LLC

Isn't DLP The Same As A Firewall?



- No! DLP tools and firewalls are fundamentally different
- In general, firewalls serve as buffers between two networks, typically your local network and the Internet, blocking unauthorized access from one to the other
- Firewalls do not have content monitoring capabilities and, therefore, do not analyze the data passing through for sensitivity…that's what the DLP tool does
- Both are necessary to help protect your systems and the sensitive data that resides on them

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Before Implementing DLP



- Ensure that appropriate written policies are in place regarding protecting sensitive data and that team members have been educated on why this is important and how to handle matters regarding sensitive data
- For example, if a customer or client calls and asks for an email of a PDF copy of a document that contains sensitive information, how is the team member to respond?
  - Delicate balance of customer/client service versus security

Copyright 2026, K2 Enterprises, LLC

Before Implementing DLP



- Additionally, ensure that appropriate tools are in place to allow team members to respond to requests and needs, such as the one identified previously
- In that specific case, is a secure portal a viable option? What about encrypted email? What about simply encrypting the PDF document with a password? What other options exist to satisfy the customer/client without unduly burdening either party and while providing an exceptional level of service?

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



HOW DO I CREATE AND IMPLEMENT DLP RULES TO HELP PROTECT SENSITIVE DATA?

Copyright 2026, K2 Enterprises, LLC

Implementing DLP In Microsoft 365



- Many business professionals today have email provided through Exchange Online accounts, often as part of their Microsoft 365 subscription
- Administrative users can create and deploy DLP rules, provided the organization has a Plan 2 Exchange account, which includes Microsoft 365 E3 and E5
- A good place to start is http://bit.ly/2IMnSGu

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Summary Of DLP Tools



- Establishing policies and training end-users is still a vital aspect of information security
- However, let's recognize the human element and understand that mistakes – some honest and some intentional – will be made that compromise the security of sensitive data
- This is where DLP kicks in and blocks the outflow of data before we have a significant breach
- Given the relatively low cost and ease of implementation, what is holding us back?

Copyright 2026, K2 Enterprises, LLC



FIVE COMMON SENSE STEPS TO SECURING YOUR PC

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Five Common Sense Steps



Control Access to Devices and Data

Restrict Assignment of Administrative Rights

Block USB Ports from Data Transfer

Encrypt Your Disk Drives

Use “Whitelists” to Manage Applications

Copyright 2026, K2 Enterprises, LLC

Control Access To Computer, Applications, & Data



- Physical access
- Strong passwords (SANS Institute)
  - At least 12 alphanumeric characters
  - Both upper and lower-case letters
  - At least one number (for example, 0-9)
  - At least one special character (ex: !$%^&*()_+|~-=\`{}[]:";'<>?,/)
  - Not written down
  - Never recycled

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

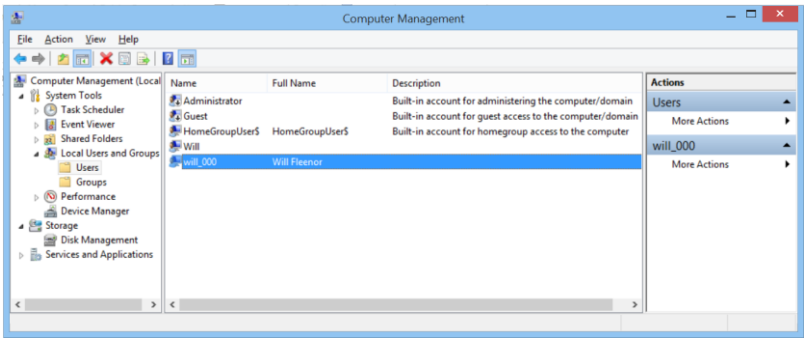
Restrict Administrative Rights

- Prevents accidental changes to security settings
- Prevents Web pages from installing code
- Provides control whenever software is installed
- Blocks execution many malware titles
- Administrative password required to install software

Copyright 2026, K2 Enterprises, LLC

Restricting Administrative Rights

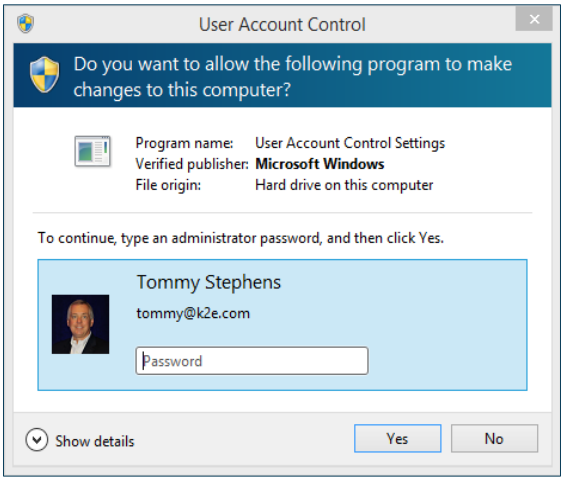
- Administrative users vs. Standard users
- User Account Control



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

User Account Control



Copyright 2026, K2 Enterprises, LLC

Block USB Ports From Data Transfer

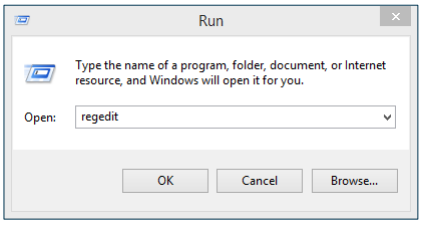
- A significant source of data leaks
  - Disgruntled employee steals valuable competitive data before being fired or quitting to move to another company
  - Data copied to flash drives for convenience then the flash drive is lost or stolen
  - Data is copied to an unencrypted external hard drive for backup and the drive is lost or stolen
- Faster, more secure methods of data transfer and backup are readily available

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Disabling USB Data Transfer

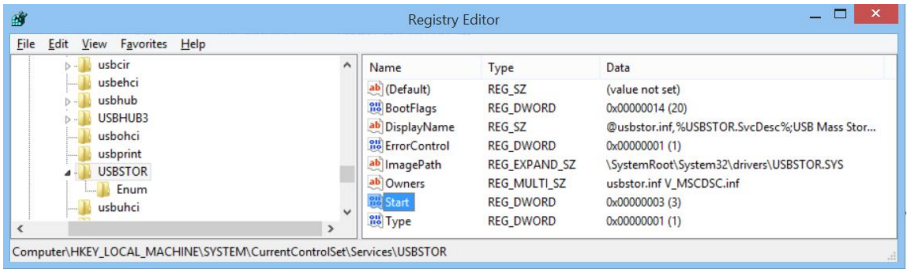
- Modifying the Registry to control USB data transfer
- Run **Regedit** from the Run Dialog Box
- Always backup the Registry before editing



Copyright 2026, K2 Enterprises, LLC

Disabling USB Data Transfer

- Modifying Registry requires administrative rights
- Change setting as described in outline
- This change does not impact other USB devices, such as mice, keyboards, scanners, etc.



Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Encrypt Your Disk Drives



- A must for laptops with sensitive data
- 47 states have security breach notification laws
- Reporting a breach can be expensive
  - Generally, reported in the range of $145 to $250 per person
- Encryption of data provides safe harbor in most states
- File level vs. whole disk encryption

Copyright 2026, K2 Enterprises, LLC

Encrypting With Windows BitLocker

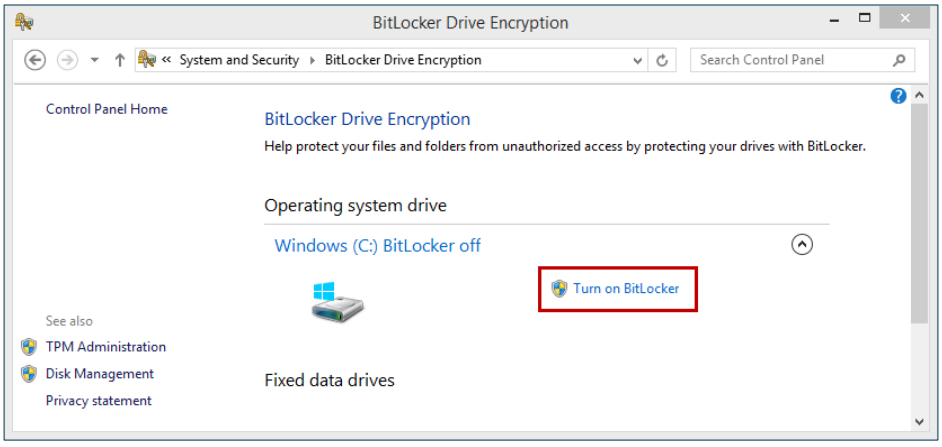


- Available free in the following versions of Windows
  - Windows Vista – Ultimate, Enterprise
  - Windows 7 – Ultimate, Enterprise
  - Windows 8/8.1 – Pro, Enterprise
  - Windows Server 2008 and newer
  - Windows 10/11 selected editions
- Found in **Control Panel** under **System and Security**

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Encrypting With Windows BitLocker



Copyright 2026, K2 Enterprises, LLC

Whitelisting Apps With AppLocker

- Business-oriented versions of Windows offers **AppLocker** to create “whitelists”
- Works on a single computer or with Windows Active Directory
- AppLocker can enhance PC security in the following areas:
  - Prevent malicious software (malware) and unsupported applications from being installed
  - Prevent users from installing and using unauthorized applications
  - Implementing application control policies for security policy and other compliance requirements

Copyright 2026, K2 Enterprises, LLC

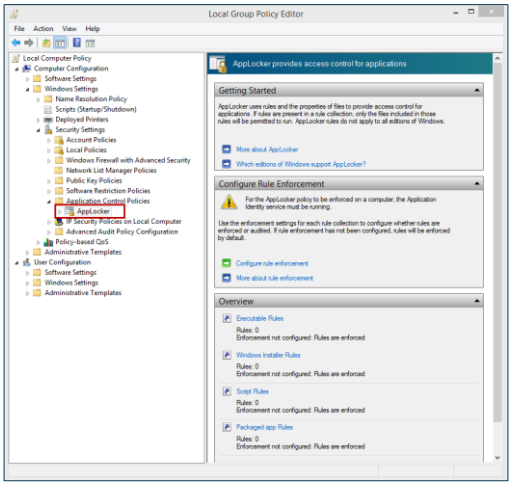
Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Configuring AppLocker

- Make a full system backup before enabling AppLocker!
- Make sure the Application Identity service is running
- Follow these steps:
  - Enter **gpedit.msc** in the Run dialog box
  - In the Local Group Policy Editor navigate to
    Windows Settings - Security Settings - Application Control Polices
  - Click **AppLocker**

Copyright 2026, K2 Enterprises, LLC

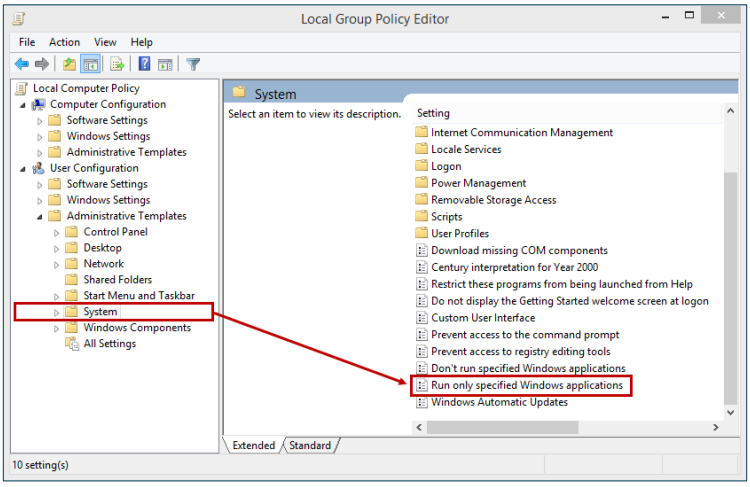
Configuring AppLocker



K2 Enterprises
Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Creating A Whitelist With Group Policy



Copyright 2026, K2 Enterprises, LLC

OTHER IMPORTANT SECURITY TOOLS YOU SHOULD CONSIDER

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

WHAT DOES THE IRS HAVE TO SAY?

Copyright 2026, K2 Enterprises, LLC

As Most Practitioners Know…

- The IRS **MANDATES** a Written Information Security Plan (**WISP**) for all firms preparing tax returns
- The fundamental requirements of such a plan include six specific items

1. Objective, purpose, and scope
2. Designated responsible individuals
3. Risk assessment
4. Hardware Inventory
5. Security safeguards, such as MFA, Data Breach response plan, etc.
6. Implementation clause confirming that the plan was implemented in compliance with GLBA and Safeguards Rule

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Becoming More Anonymous



- Consider setting up an anonymous server or using private sessions in web browsers
- You could – perhaps should – use personal VPNs such as **Private Internet Access** or **Nord**
- Also, your choice of browser matters…some consider **Opera** and **Firefox** to be more secure and more private…**TOR** is widely regarded as the most secure and private browser
  - Another good browser option is **Brave**
- Don't forget search engines…**DuckDuckGo** is widely regarded as the most private search engine

Copyright 2026, K2 Enterprises, LLC

Security Tools - Firewalls



- Required in virtually all businesses and some homes
- Need to keep security services up to date, to be updated continuously
- At times, there may be a major configuration change to mitigate new threats and strategies
- Must be powerful enough to run security suites for integrated intrusion prevention service (IPS) – SonicWall or WatchGuard
- Should maintain a DMZ for non-secure portions of your network
- In some cases, home grade firewalls/routers may not provide enough protection and are rarely updated for discovered security vulnerabilities

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

Security Tools – AntiMalware Tools



- Signature based spam control (Vipre) is not as effective as heuristic products (Webroot)
- Needs to be updated at least daily, but you may want to sandbox new signatures for 24 hours
- Better if controlled from a single management console where client detections are reported to network administrators
- Users should not be permitted to attach to your networks if their AV signature is out of date

Copyright 2026, K2 Enterprises, LLC

Security Tools – Backup



- As odd as it sounds, backup is one of your best protections
  - Continuous or no more than 15-minute increments
  - Tested
  - Store a copy off-site
- It's not a matter if you'll be infected, but when
- Confirm you have what you think you have!
  - If you're in the cloud, refer to your license agreement, and ask for proof of tests
  - Better yet, schedule a regular test or reverse backup
  - Premise – best approach we know is to use a backup appliance

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.

SUMMARY

Copyright 2026, K2 Enterprises, LLC

Security Summary

- Security risks abound and grow by the day
- This leaves many feeling that security is a lost cause
- In fact, although we live and work in a risky world, there are key steps that we can take to manage the risks to us and our data
- Identify the key risks affecting your organization, train your team, and implement the specific internal controls you need to mitigate that risk to a prudently acceptable level
- And remember, this is a process, not a one-time project…update and revise your protocols as your risks evolve

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.



THANKS!

Copyright 2026, K2 Enterprises, LLC

Copyright © 2026, K2 Enterprises, LLC.
Reproduction or reuse for purposes other than a K2 Enterprises training event is prohibited.