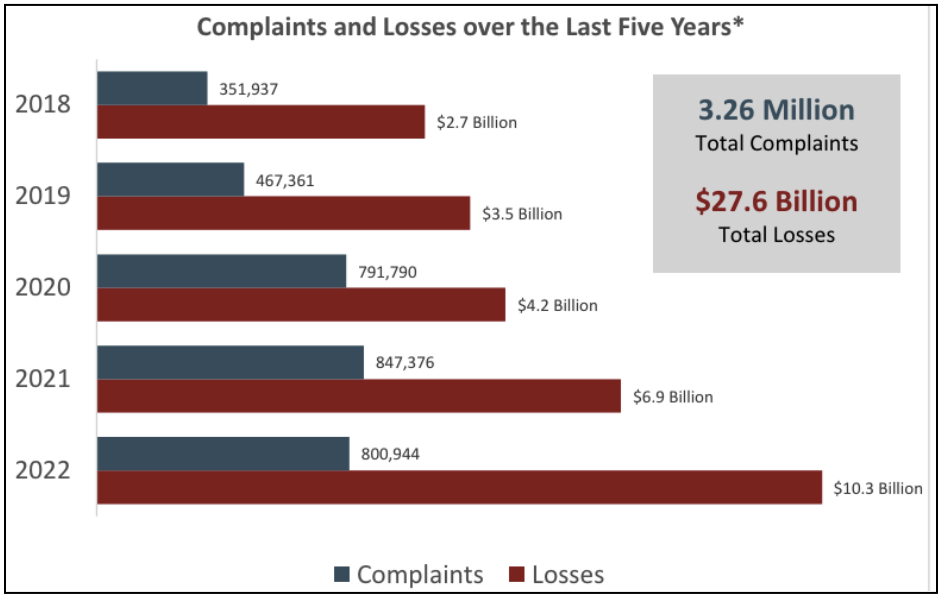
Business Hacks and Attacks Stats

How can you prevent such attacks and hacks?

Implement robust cybersecurity measures and continual employee training, to identify vulnerabilities and prevent becoming a victim.

See more stats and references here: tronpilottech.com/fraud-prevention/

Ref: FBI 2022 Internet Crime Report (stats are based ONLY on reported incidents)



Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
1	Imposter Scams	176,327	24%	$645.7M	$780
2	Online Shopping and Negative Reviews	79,850	79%	$88.7M	$119
3	Business and Job Opportunities	27,403	33%	$134.0M	$2,000
4	Internet Services	24,172	29%	$33.3M	$299
5	Investment Related	23,270	80%	$1,105.9M	$9,646
6	Telephone and Mobile Services	20,277	41%	$14.0M	$265
7	Health Care	16,395	53%	$16.0M	$258
8	Travel, Vacations and Timeshare Plans	10,729	69%	$49.5M	$995
9	Prizes, Sweepstakes and Lotteries	9,339	29%	$46.7M	$600
10	Mortgage Foreclosure Relief and Debt Management	7,781	22%	$17.7M	$1,250

Ref: FTC Consumer Sentinel Network Report published Apr 25, 2024

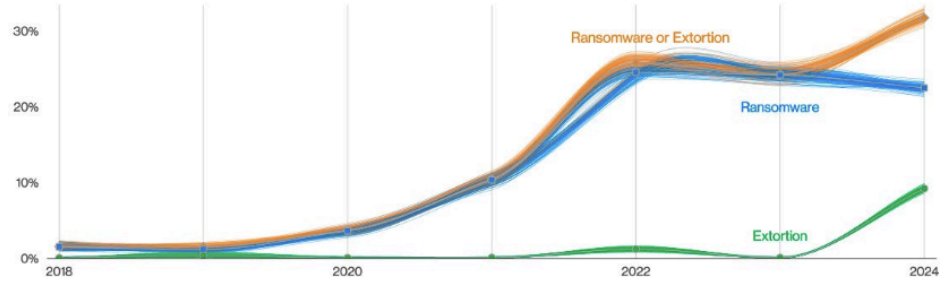


Figure 2. Ransomware and Extortion breaches over time

Ref: Verizon 2024 Data Breach Investigations Report

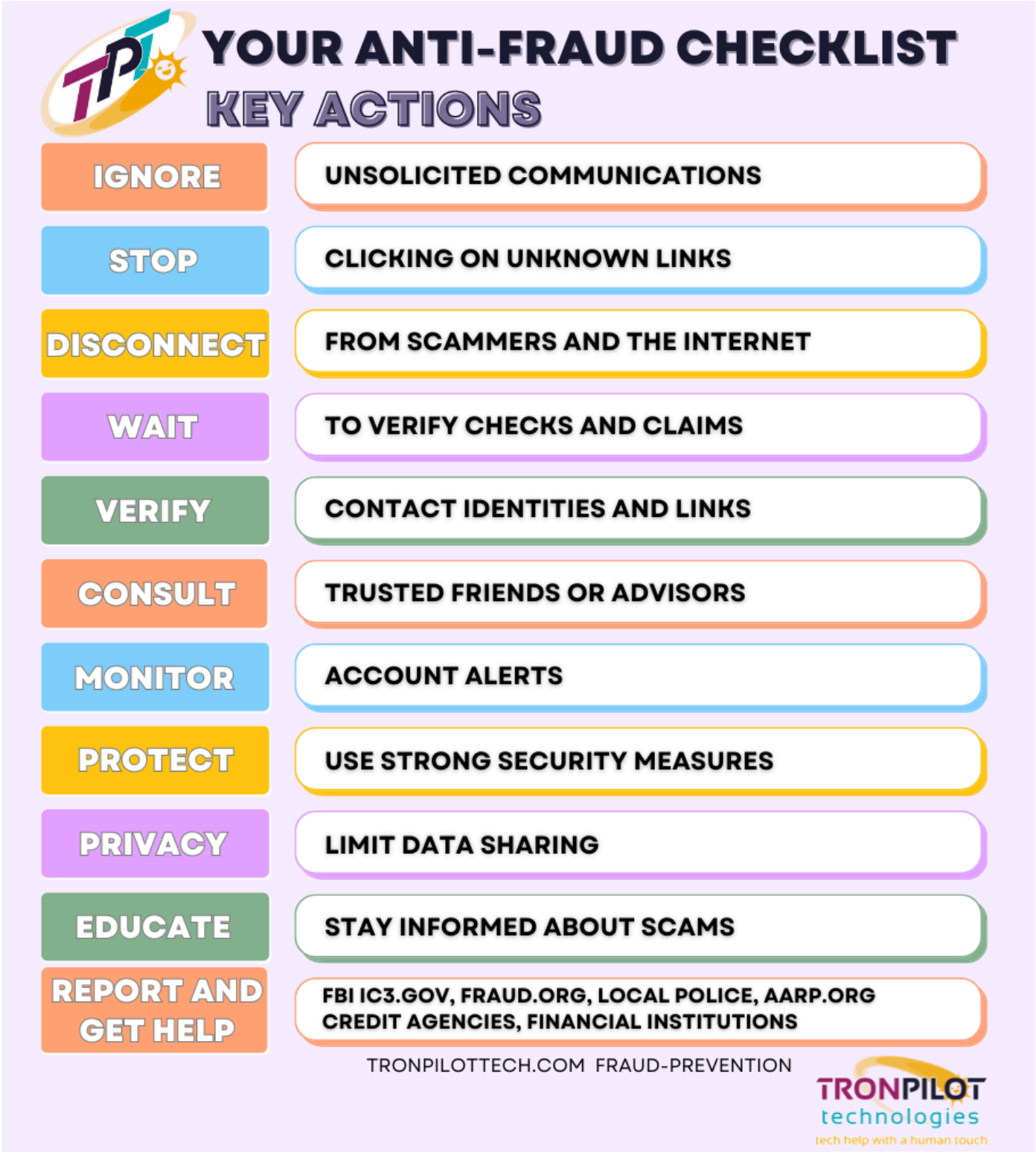
USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

Ref: IBM Cost of a Data Breach Report 2023

Real-world examples of news-worthy breaches, hacks, and ransomware incidents that affected businesses in the past year, highlighting the diverse attack methods and significant impacts.

Incident	***Impact***
GoDaddy Multi-Year Breach (Discovered 2023)	Allowed attackers to steal source code and install malware, affecting 1.2 million Managed WordPress customers, leading to data loss and reputational damage, with extensive costs on investigation and remediation. https://www.bleepingcomputer.com/news/security/the-biggest-cybersecurity-and-cyberattack-stories-of-2023/
PayPal Invoice Scam	Fake invoices sent through PayPal, impersonating brands like Norton and McAfee. Numerous businesses experienced financial losses and system compromises. Contact info on invoices went to scammers, who directed install of remote access tools, further compromising clients. https://www.intego.com/mac-security-blog/fake-invoice-scams-norton-mcafee-paypal/
MOVEit Transfer Vulnerability Exploitation (June 2023)	Affected numerous organizations, including Shell and the BBC, leading to data breaches and significant operational disruptions. Kaspersky Blog - https://www.kaspersky.com/blog/the-biggest-ransomware-attacks-of-2023/
Bluefield University Ransomware Attack (May 2023)	Hijacked the university's emergency alert system, threatening to release stolen data and causing examination postponements. https://www.cm-alliance.com/may-2023-recent-cyber-attacks-data-breaches-ransomware-attacks
Topgolf Callaway Data Breach (Sept 2023)	Exposed sensitive customer information, leading to identity theft and loss of customer trust. Tech.co - https://tech.co/news/data-breaches-2024
City of Dallas Ransomware Attack (May 2023)	Affected several municipal services, including the police department's IT systems, causing disruptions in public services and significant recovery costs. Kaspersky Blog - https://www.kaspersky.com/blog/the-biggest-ransomware-attacks-of-2023/ Cyber Management Alliance - https://www.cm-alliance.com/may-2023-recent-cyber-attacks-data-breaches-ransomware-attacks
23andMe Data Breach (Oct 2023)	Exposed personal and genetic data of users, leading to identity theft and loss of customer trust. Tech.co - https://tech.co/news/data-breaches-2024
MGM Resorts Cyber Attack (Sept 2023)	Disrupted various IT systems, including in-casino services and online reservations, causing significant operational and financial losses in the millions. Bleeping Computer - https://www.bleepingcomputer.com/news/security/the-biggest-cybersecurity-and-cyberattack-stories-of-2023/
Tesla Insider Data Leak (May 2023)	Exposed data on customers, employees, and business partners, leading to potential identity theft and significant reputational damage. Cyber Management Alliance - https://www.cm-alliance.com/may-2023-recent-cyber-attacks-data-breaches-ransomware-attacks
Toronto Public Library Ransomware Attack (Nov 2023)	Stolen sensitive personal information of employees, customers, and volunteers, leading to identity theft and a loss of trust. Tech.co - https://tech.co/news/data-breaches-2024
Reddit Ransomware Attack (Feb 2023)	Obtained unauthorized access to corporate documents and code, leading to data leaks and significant operational disruptions. Heimdal Security - https://heimdalsecurity.com/blog/recent-ransomware-attacks-ransoms-consequences-and-more/
San Francisco's Bay Area Rapid Transit (BART) Attack (Mar 2023)	Exposed sensitive data, causing operational disruptions and potential identity theft. Heimdal Security - https://heimdalsecurity.com/blog/recent-ransomware-attacks-ransoms-consequences-and-more/
Tallahassee Memorial HealthCare Ransomware Attack (Feb 2023)	Caused significant operational disruptions, including switching to paper documentation and limiting surgeries and procedures. Heimdal Security - https://heimdalsecurity.com/blog/recent-ransomware-attacks-ransoms-consequences-and-more/
Technion Institute of Technology Ransomware Attack (Feb 2023)	Demanded a $1.7 million ransom, impacting the university's operations and data integrity. Heimdal Security - https://heimdalsecurity.com/blog/recent-ransomware-attacks-ransoms-consequences-and-more/



Download the Detailed Version with Explanations & Resources here:

https://www.tronpilottech.com/fraud-prevention/

Your Anti-Fraud Checklist

🚫 Ignore:

- ☐ Ignore unsolicited calls, emails, texts, and social media messages.
- ☐ Respond only to known contacts. If unsure, always verify!

🛑 Stop:

- ☐ Do not click on pop-ups, links, or attachments from unknown sources.
- ☐ Do not contact numbers provided in unsolicited messages.
- ☐ Do not give control of your computer to unknown individuals.
- ☐ Do not share personal information over the phone unless you initiated the call to a verified number.

🔌 Disconnect:

- ☐ End communication with suspected scammers.
- ☐ Disconnect from the internet and shut down your device if you see suspicious pop-ups or locked screens.
- ☐ Avoid opening email attachments from unknown senders.

⏳ Wait:

- ☐ Resist pressure to act quickly; take your time to verify the situation.
- ☐ Wait for checks to clear before acting on them to avoid overpayment scams.

✔️ Verify:

- ☐ Independently verify the identity of contacts by looking up their official contact information.
- ☐ Only download apps and software from verified, trusted sources.

👥 Consult:

- ☐ Discuss unusual communications with trusted friends or advisors.
- ☐ Research online for reports of similar scams.

📈 Monitor:

- ☐ Set up alert notifications for transactions and changes in your online accounts.
- ☐ Verify alerts for any transactions you make.

🔒 Protect:

- ☐ Use strong, unique passwords for each account.
- ☐ Enable multi-factor authentication (MFA).
- ☐ Keep software and systems updated.
- ☐ Use secure Wi-Fi and ensure your home Wi-Fi has a strong password.
- ☐ Use reputable anti-virus software, firewalls, and VPN services.
- ☐ Enable pop-up blockers.
- ☐ Use a credit monitoring service and place credit freezes/locks.

🛡️ Privacy:

- ☐ Adjust privacy settings on devices and online accounts to limit data sharing.
- ☐ Properly dispose of personal documents.
- ☐ Be cautious about sharing personal information; use fake details for non-essential services.
- ☐ Pre-authorize who can access your personal health information.

📚 Educate:

- ☐ Stay informed about new scams by subscribing to newsletters from AARP, FTC, NCOA, CFPB, and Fraud.org.

Business Self-Assessment Checklist

Protect Your Business from Cyber Crime

📊 Data Assessment

- ☐ Identify Critical Data:
  - ☐ What types of data are critical to your business operations?
  - ☐ Where is this data stored (local servers, cloud services, etc.)?
- ☐ Data Classification: Have you classified data based on its sensitivity (public, internal, confidential)?
- ☐ Data Access Control: Who has access to sensitive data? Are access controls in place?
- ☐ Data Encryption: Is sensitive data encrypted both at rest and in transit?

🔧 Operations Assessment

- ☐ Process Documentation: Are key business processes documented?
- ☐ Operational Dependencies: What are the critical dependencies for your operations (software, hardware, third-party services)?
- ☐ Workflow Efficiency: Are there any bottlenecks or inefficiencies in your current workflows?

💻 Tech Stack Assessment

- ☐ Inventory of Technology: Do you have an up-to-date inventory of all hardware and software used in your business?
- ☐ Software Licensing: Are all software licenses up to date and compliant?
- ☐ Hardware Maintenance: Is all hardware regularly maintained and updated?
- ☐ Technology Utilization: Are you using the full capabilities of your current tech stack?

📦 Business Continuity and Disaster Recovery Assessment

- ☐ Business Impact Analysis (BIA): Have you conducted a BIA to identify critical business functions and the impact of disruptions?
- ☐ Business Continuity Plan (BCP): Do you have a BCP in place? Is it documented and regularly updated?
- ☐ Disaster Recovery Plan (DRP): Is there a DRP for IT systems and data recovery? Are recovery time and recovery point objectives (RTO, RPO) defined?
- ☐ Regular Testing: Are BCP and DRP tested regularly through drills or simulations?

🔒 Security Practices Assessment

- ☐ Access Control: Are strong access controls implemented (e.g., MFA, least privilege)?
- ☐ Employee Training: Do employees receive regular training on cybersecurity best practices and threat awareness?
- ☐ Endpoint Security: Are all endpoints protected with up-to-date antivirus and anti-malware software?
- ☐ Network Security: Are firewalls and intrusion detection/prevention systems in place and properly configured?
- ☐ Regular Updates and Patching: Are all systems and applications regularly updated and patched?

📜 Compliance and Regulatory Assessment

- ☐ Regulatory Requirements: What regulatory requirements apply to your business (e.g., GDPR, HIPAA, PCI DSS)?
- ☐ Compliance Status: Are you currently compliant with these regulations? What gaps need to be addressed?
- ☐ Policy Documentation: Are all compliance-related policies and procedures documented and communicated to employees?

🤝 Vendor and Third-Party Risk Assessment

- ☐ Vendor Inventory: Do you have a list of all vendors and third-party service providers?
- ☐ Vendor Security: Have you assessed the security practices of your vendors? Do they comply with your security requirements?
- ☐ Contracts and SLAs: Are contracts and service level agreements (SLAs) in place and regularly reviewed?

📈 Next Steps After Assessment

- ***Quantify and Prioritize Risks:*** Based on your assessment, prioritize the most critical risks and vulnerabilities that need to be addressed.
- ***Develop an Action Plan:*** Create a detailed action plan with specific steps, responsible parties, and deadlines to address identified risks.
- ***Implement Quick Wins:*** Start with quick wins that can significantly improve your security posture with minimal effort and cost.
- ***Invest in Training:*** Ensure all employees are trained on the latest cybersecurity practices and understand their roles in protecting the business.
- ***Engage Experts:*** Consider engaging cybersecurity and IT experts to help implement complex solutions and provide ongoing support.
- ***Monitor and Review:*** Establish a process for continuous monitoring and regular review of your security practices to adapt to new threats and changes in your business environment.