ISSUE 017
December 2024
Independence, Missouri

FCS TECH TALK

Your Trusted Technology Partner Since 1989

INSIDE THIS ISSUE:

CYBERCRIME THROUGH THE YEARS: WHAT DOES THE FUTURE HOLD?

Cybercrime has evolved significantly over the past few decades, adapting to technological advancements and changing the landscape of digital security. Here is how cybercrime has effected each decade.

1980s: The Birth of Cybercrime

Cybercrime as we know it began in the 1980s with the advent of personal computers and email. Early cybercriminals used simple viruses and email scams to target individuals and businesses.

These attacks were relatively unsophisticated but laid the groundwork for more complex threats

1990s: The Rise of the Internet

The widespread adoption of the internet in the 1990s introduced new opportunities for cybercriminals. Techniques like domain spoofing and the distribution of malware through email attachments became common.

The first major cyberattacks, such as the Morris Worm in 1988, highlighted the vulnerabilities of interconnected systems.

2000s: Social Media and Identity Theft

The 2000s saw the rise of social media, which provided cybercriminals with a wealth of personal information. Identity theft became rampant as people shared more of their lives online. Phishing attacks, where attackers trick individuals into revealing sensitive information, became more sophisticated and widespread.

2010s: Advanced Persistent Threats (APTs)

In the 2010s, cybercrime evolved into a more organized and professional activity. Advanced Persistent Threats (APTs) emerged, involving prolonged and targeted attacks often backed by nation-states.

These attacks aimed at stealing intellectual property, financial data, and other sensitive information from businesses and governments.

2020s: The Era of Ransomware and Automation

The 2020s have been marked by a surge in ransomware attacks, where cybercriminals encrypt a victim's data and demand a ransom for its release.

The COVID-19 pandemic accelerated the shift to remote work, increasing vulnerabilities and leading to a 300% rise in cybercrime since March 2020.

Automation has also become a key tool for both attackers and defenders, with automated attacks becoming more common and sophisticated.

Impact on Small Businesses

Increased Targeting of Small Businesses Small businesses have become prime targets for cybercriminals due to their often weaker security measures compared to larger corporations.

A recent survey found that 41% of small businesses were victims of a cyberattack in 2023. Cybercriminals exploit the often limited knowledge and protection for small businesses who often over look large security vulnerabilities.

Most Common Threats to Small Businesses Today

Ransomware: Small businesses are frequently targeted by ransomware attacks, which can halt operations and lead to significant financial losses.

Business Email Compromise (BEC): BEC attacks involve impersonating high-level executives or vendors to trick employees into transferring funds or revealing sensitive information.

Phishing: Phishing remains a prevalent threat, with attackers using deceptive emails to steal credentials and other sensitive data.

Future Trends in Cybercrime

Artificial Intelligence (AI) and Machine Learning (ML)

AI-Powered Attacks: Cybercriminals will increasingly use AI and ML to launch more sophisticated and targeted attacks. AI can automate the process of finding vulnerabilities and launching attacks, making it easier for cybercriminals to breach systems.

Defensive AI: On the flip side, AI will also be used to enhance cybersecurity defenses, with AI-driven systems capable of detecting and responding to threats in real-time.

Internet of Things (IoT) Vulnerabilities

Connected Devices: As more devices become interconnected, the attack surface for cybercriminals expands. IoT devices often lack robust security measures, making them prime targets for attacks.

Botnets: Cybercriminals can hijack IoT devices to create botnets, which can be used to launch large-scale Distributed Denial of Service (DDoS) attacks.

Ransomware Evolution

Ransomware-as-a-Service (RaaS): The rise of RaaS platforms allows even non-technical criminals to launch ransomware attacks by purchasing ready-made ransomware kits.

Double Extortion: Future ransomware attacks may involve not only encrypting data but also threatening to release sensitive information publicly if the ransom is not paid.

Example of a Future Cyberattack:

Imagine a small business that relies heavily on IoT devices for its operations, such as smart thermostats, security cameras, and inventory management systems.

In the near future, a cybercriminal could use AI to scan for vulnerabilities in these IoT devices. Once a vulnerability is found, the attacker could deploy malware to take control of the devices, creating a botnet.

The attacker then uses this botnet to launch a DDoS attack against the business's website, causing it to crash and disrupting operations.

Simultaneously, the attacker deploys ransomware to encrypt the business's critical data and demands a ransom in cryptocurrency. To increase pressure, the attacker threatens to release sensitive customer information if the ransom is not paid.

Preventive Measures:

Regular Security Audits: FCS can help conduct regular security audits of all devices to identify vulnerabilities on your network. Once identified these vulnerabilities can be quickly updated or replaced depending on the device.

Implement EDR + 24/7 SOC: Security services like an EDR paired with a Security Operations Center (SOC) create an almost bullet proof operation, alerting you of any malicious activity on all network devices and launching remediation immediately.

Incident Response Plan: FCS can help develop and regularly update an incident response plan for you to quickly address and mitigate the impact of cyberattacks.

ISSUE 017
December 2024
Independence, Missouri

THIS MONTH'S PRODUCT SPOTLIGHT

CLICK HERE FOR MORE INFO!

BLOCK IMPERSONATORS

REMOVE PHISHING ATTEMPTS

ADVANCED EMAIL PROTECTION

FILTER SPAM EMAILS

BLOCK RANSOMWARE

HOW PASSWORD MANAGERS PROTECT YOUR ACCOUNTS

A password manager keeps all your passwords in one place. Think of it as a digital safe for your login information.

You only need to remember one password, the master password. This master password lets you access all your other passwords.

Types of Password Managers

- Apps you download on your phone or computer
- Tools that work in your web browser
- Some offer both options

Why Use a Password Manager?

- It Helps You Create Strong Passwords. Password managers generate long, random passwords that are hard to crack.
- It Remembers Your Passwords. With a password manager, you don't need to memorize many passwords. The tool does this for you.
- It Keeps Your Passwords Safe. Password managers use high-level security to protect your data. Even if someone hacks the password manager company, they can't read your information.

Features of Password Managers

- Password Generation: Good password managers can create tough, unique passwords for you.
- Auto-Fill: Many password managers can fill in your login information on websites. This saves time and avoids typos.
- Secure Notes: Some password managers let you store credit card numbers or important documents.
- Password Sharing: Some tools let you share passwords safely with family or coworkers.

How to Choose a Password Manager

- Find one with strong encryption and two-factor authentication.
- The manager should be easy for you to understand and use.
- Make sure it works on all your devices.
- Research the features you want and the price you can afford.

Consider using a password manager today to improve your online security. If you need help choosing or setting up a password manager, contact us today.

DO YOU REALLY NEED DARK WEB MONITORING?

Dark web monitoring looks for your information on the dark web. It can find stolen passwords or credit card numbers. This helps you know if someone stole your data.

But is dark web monitoring really necessary? Here are the most important benefits to consider:

• Identity and business protection.
It helps you know if someone stole your personal or business data. You can then change passwords and protect yourself.

• AI monitoring to spot patterns that people might miss.
AI helps them search faster and better.

• Real-time alerts when your information is stolen.
The tools send an alert right away when they find your information.

• Protection for passwords, credit card numbers, social security numbers, and more.
This enables you take quick, specific actions.

Dark web monitoring is an easy way to protect your information. It watches when you can't. If you want to stay safe online, it's a good tool to have.

YEAR-END REVIEW OF DATA BREACHES IN 2024

As 2024 draws to a close, the year's landscape of data breaches underscores the persistent and evolving challenges of cyber security. From sophisticated ransomware attacks to large-scale data exposures, organizations worldwide have faced significant threats that highlight both vulnerabilities and the need for robust defenses.

Key Trends in 2024

1. Rise in AI-Driven Attacks: The widespread adoption of artificial intelligence (AI) has been a double-edged sword. While AI has empowered cybersecurity teams with advanced threat detection capabilities, it has also been weaponized by cybercriminals. AI-driven phishing campaigns, capable of mimicking human-like communication, have increased in sophistication, deceiving even the most vigilant users.

2. Targeting Critical Infrastructure: In 2024, critical infrastructure sectors such as energy, healthcare, and transportation were prime targets for cyberattacks. Threat actors exploited outdated systems and weak points in supply chains to disrupt services and demand hefty ransoms. These incidents underscored the urgent need for cybersecurity upgrades in essential services.

3. Focus on Small and Medium Enterprises (SMEs): SMEs faced a disproportionate number of attacks due to their limited cybersecurity resources. Ransomware groups shifted their focus to these organizations, knowing they were more likely to pay ransoms to resume operations quickly.

Notable Incidents

1. Global Retail Breach: In March 2024, a major global retailer suffered a data breach exposing over 500 million customer records. The breach was traced to a compromised third-party vendor, highlighting the risks associated with supply chain vulnerabilities.

2. Healthcare Ransomware Attack: A ransomware attack in July targeted a leading healthcare provider, encrypting patient data and disrupting services across multiple facilities. The attackers demanded $50 million in cryptocurrency, bringing patient care to a halt for weeks.

3. Government Agency Hack: In October, a national government agency's systems were infiltrated by an advanced persistent threat (APT) group. Sensitive intelligence data was exfiltrated, sparking widespread concerns about national security and international relations.

Lessons Learned

1. Strengthen Supply Chain Security: Third-party vendors remain a weak link in many organizations' cybersecurity defenses. Rigorous vetting, continuous monitoring, and contractual requirements for security measures are essential to mitigate these risks.

2. Prioritize Employee Training: Human error continues to play a significant role in data breaches. Comprehensive and regular training on recognizing phishing attempts and practicing good cyber hygiene is critical.

3. Invest in Incident Response: Having a robust incident response plan can minimize the impact of a breach. Organizations that practiced and updated their response plans recovered more quickly and at a lower cost.

The Road Ahead

Looking forward to 2025, organizations must prepare for an increasingly complex threat landscape.

Cybersecurity should be viewed not as an expense but as a critical investment. Collaboration between governments, private organizations, and cybersecurity experts will be vital to counter emerging threats.

By learning from 2024's breaches and implementing proactive measures, businesses can better safeguard their data, maintain customer trust, and ensure resilience in the digital age.

ISSUE 017
December 2024
Independence, Missouri

TECHNOLOGY TRENDS TO WATCH IN 2025

As we approach 2025, technology continues to advance at a breakneck pace, reshaping industries, redefining work, and transforming everyday life.

From artificial intelligence (AI) breakthroughs to innovations in sustainability, here are the key trends expected to dominate in 2025.

1. AI-Driven Everything

AI will extend its reach across nearly every sector, enabling smarter automation, personalization, and decision-making. Generative AI, like ChatGPT, will further mature, offering capabilities that blend creativity with functionality. In 2025, expect:

- AI Co-Pilots: Integrated AI assistants embedded in tools and platforms, guiding professionals across industries from coding to healthcare.
- Responsible AI: Enhanced efforts to create transparent, ethical, and unbiased AI systems as global regulations catch up with technology.
- Hyper-Personalization: AI-driven recommendations tailored to individual preferences in education, e-commerce, and entertainment.

2. Quantum Computing Breakthroughs

Quantum computing, long seen as a futuristic concept, will gain traction in 2025. Companies will move from experimental phases to practical applications, particularly in sectors like:

- Drug Discovery: Accelerating research for new treatments by simulating molecular interactions.
- Supply Chain Optimization: Solving logistical challenges with unprecedented speed.
- Cryptography: Advancing encryption methods to counter potential quantum threats.

3. Next-Gen Connectivity with 6G

While 5G continues to expand globally, the groundwork for 6G will solidify. With speeds up to 100 times faster than 5G and near-zero latency, 6G promises:

- Immersive XR Experiences: Seamless integration of virtual, augmented, and mixed reality into everyday life.
- Smart Cities: Enhanced IoT networks enabling real-time traffic management, energy optimization, and public safety.
- Holographic Communication: Real-time, high-resolution holograms for remote meetings and events.

4. Sustainability Tech Takes Center Stage

Sustainability will no longer be optional as consumers and governments demand greener practices. In 2025, technology will focus on:

- Clean Energy Innovations: Advances in solar, wind, and battery storage to power a renewable future.
- Circular Economies: AI and IoT-enabled systems that track and optimize resource usage, reducing waste.
- Carbon Capture Technologies: Scaling solutions to remove CO_2 from the atmosphere effectively.

5. The Rise of BioTech and Human Augmentation

Biotechnology will continue to push boundaries in healthcare and beyond. Key developments include:

- Personalized Medicine: Tailoring treatments based on individual genetic profiles.

6. Cyber Security in the Spotlight

As technology grows more complex, so do cyber threats. 2025 will emphasize:

- AI-Powered Security: Proactive threat detection using machine learning.
- Zero-Trust Architectures: Strengthening systems by assuming no implicit trust within networks.
- Biometric Authentication: Moving beyond passwords to more secure, user-friendly solutions.

7. Edge Computing and Decentralized Systems

With the explosion of IoT devices, edge computing will reduce latency by processing data closer to its source. In 2025, expect:

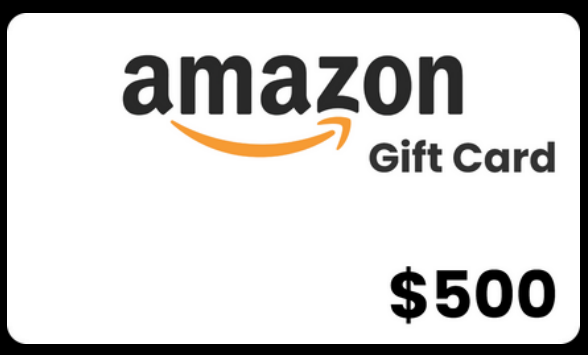
- Decentralized AI: AI models trained and deployed locally on devices rather than relying on centralized servers.
- Smarter IoT Devices: Enhanced functionality for smart homes, factories, and cities.
- Energy-Efficient Systems: Lower power consumption in data processing.

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to another business in need of IT services. Referrals help us keep costs down so we can pass the savings to our clients.

If your referral ends up becoming a client - we'll gift them their first month of service at no charge AND we'll gift you a $500 Amazon Gift Voucher.

Simply introduce me via email to stan@fcskc.com and I'll take it from there. I personally promise we'll look after your referral's business with a high level of care and attention (just like we do with all our clients).
-Stan



We Want Your Feedback

Here at Ferguson Computer Services, we value your feedback greatly and would appreciate if you took time from your busy schedule to leave us a review. These reviews let us know what we are doing well and what we might be able to improve on in the future.

Leave a Google Review Leave a Facebook Review

TECHNOLOGY TRIVIA TIME

Technology Trivia Question of the Month! Send the correct answer to winner@fcskc.com to be entered to win a $50 gift card to Amazon.

Here is December's question of the month: What cybercrime techniques were used in the 1990's?