IN.gov

# Safeguarding Digital Presence: Analyzing Website Defacement, Its Ramifications, and Security Best Practices

June 30th, 2023

*The IN.gov Program, a partnership between the State of Indiana and Tyler Indiana, is responsible for the design, development, and maintenance of more than 330 State websites and 125 online services. Providing services for Indiana government partners for more than 25 years, the IN.gov Program continues to bring digital innovations to the state, receiving more than 100 awards in the past 4 years.*

IOT Indiana Office of Technology
Powering a State that Works

www.in.gov/iot

In today's digital age, it is common for websites to fall victim to cyberattacks. Bad actors carry out these attacks to deface websites, steal sensitive information, or cause other damage. The IN.gov program, managed by the Indiana Office of Technology (IOT), is a central hub for managing Indiana State agency websites and some Local Government websites. It also serves as a trusted resource for best practices for those governments. In this whitepaper, we will discuss why sites get defaced, the impact of defacement, and best practices to protect your website.

## Understanding website defacement

Website defacement refers to an attacker's unauthorized modification of a website's content. In most cases, the attacker gains access to the website's backend and modifies the content to display their message or image. This attack is often carried out by individuals or groups who want to spread a particular message, cause disruption, or gain notoriety. The following details potential reasons why a bad actor would target a government website:

1. **Political motivation:** Hackers may target government websites to express political dissent or promote their ideological agenda.
2. **Data theft:** Government websites can store sensitive information, such as citizen data, financial records, or classified documents, making them attractive targets for hackers seeking to steal valuable data.
3. **Disruption of services:** Attacking government websites can disrupt essential services provided to citizens, causing inconvenience and potentially compromising public safety.
4. **Espionage:** State-sponsored hackers may target government websites to gather intelligence or gain insight into government operations, policies, or sensitive information.
5. **Activism:** Hacktivist groups may target government websites to protest government actions or policies, using defacement as a means to gain attention and promote their cause.
6. **Reputation damage:** Defacing government websites can tarnish the reputation of government institutions and undermine public trust in the government's ability to secure and protect sensitive information.
7. **Financial gain:** Hackers may seek financial gain by defacing government websites and demanding ransom or exploiting vulnerabilities to gain unauthorized access to financial systems.
8. **Demonstrating technical prowess:** Some hackers target government websites to showcase their hacking skills and establish credibility within the hacker community.

*One example of a prominent website defacement is the attack on a high-profile US government website in 2015. The attackers, allegedly associated with the Islamic State, gained access to the website's backend and replaced the homepage with a message that read, "I love you ISIS". This incident caused a great deal of embarrassment for the US government, and highlighted the need for improved website security measures.*

9. **Manipulation of public perception:** By defacing government websites, hackers can manipulate public perception or spread false information, leading to confusion and potentially influencing public opinion.
10. **Retaliation or revenge:** Hackers may target government websites as an act of retaliation for perceived injustices or as revenge against specific individuals or government agencies.

## Impact of website defacement

The impact of website defacement can be significant and long-lasting. In addition to causing embarrassment and reputational damage, website defacements can also result in financial losses, especially if attackers steal sensitive information or the website is taken offline for an extended period. According to a recent study conducted by a leading provider of website security services, 68% of all websites are vulnerable to some form of attack. This means that most websites risk being defaced by bad actors who exploit these vulnerabilities to gain unauthorized access. The outcome associated with a bad actor breaching your website could be catastrophic to your organization. Risks include, but are not limited to:

1. **Reputational damage:** A defaced website can severely damage the organization's reputation, losing public trust and credibility.
2. **Information exposure:** Breaches can result in the exposure of sensitive data, including personal information, financial records, or classified documents, potentially leading to identity theft or other malicious activities.
3. **Service disruption:** A defaced website may become unavailable or experience disruptions, preventing users from accessing important services or information.
4. **Legal consequences:** If sensitive information is compromised or regulations are violated, government agencies may face legal consequences, including fines, lawsuits, or investigations.
5. **Financial losses:** Website breaches can result in financial losses due to costs associated with incident response, recovery, legal actions, and potential damages or compensations to affected parties.
6. **Compromised user trust:** Users relying on government websites may lose trust in the organization's ability to protect their data, leading to reluctance to use online services or share sensitive information.

*An example of the financial impact of website defacement is the 2013 attack on the South Korean banking industry. The attackers defaced the websites of several major banks, causing significant disruptions to online banking services. The attack resulted in millions of dollars in lost revenue and highlighted the need for improved cybersecurity measures.*

7. **Operational inefficiencies:** Dealing with a defacement or breach requires significant resources and time, diverting attention from regular operations and hindering productivity.
8. **Damage to critical infrastructure:** If the breached website is an essential part of the infrastructure, such as emergency services or utility providers, the consequences can extend to compromising public safety or disrupting critical services.
9. **Insider threats:** Website breaches can involve insider threats, where employees or trusted individuals with access to sensitive information intentionally or unintentionally contribute to the breach.
10. **Extended impact:** A website breach can have long-lasting consequences, such as reputational damage persisting even after the breach is resolved, ongoing legal battles, or lingering effects on user confidence and trust.

*Another example of the impact of defacement is the 2011 attack on a leading global video game publisher, which resulted in the theft of millions of users' personal information, including credit card numbers. The attackers defaced the website's homepage with a message that read, "We are legion." The attack resulted in multiple governments investigating the publisher's handling of the situation, significant financial losses for the publisher, and damage to the company's global reputation.*

## Best Practices to Protect Your Website

Website defacement is a serious problem that affects most websites at some point. Bad actors who seek to spread their message or cause disruption can easily exploit vulnerabilities in website security to gain unauthorized access. The impact of website defacement can be significant and long-lasting, as defacement can result in financial losses and reputational damage. Website owners must take steps to improve their website security and prevent unauthorized access by bad actors. This can include implementing strong passwords, regularly updating software, and using website security services.

The following tools and tactics can be leveraged today to help secure your website, each of which IOT uses to help protect Indiana government websites.

1. **OWASP:** The Open Web Application Security Project (OWASP) is a nonprofit organization dedicated to improving software security. Their website offers a wealth of information on website security, including best practices and guides for secure development.
2. **Sucuri:** Sucuri is a website security company offering various services to protect websites from attacks. They offer website scanning, malware removal, and firewall protection.
3. **Google Search Console:** Google Search Console is a free tool provided by Google that allows website owners to monitor their website's performance in Google search results. It also provides alerts for security issues and manual actions taken against the website.

4. **HTTPS:** HTTPS is a secure version of HTTP, the protocol for transmitting data over the internet. Websites that use HTTPS encrypt all data transmitted between the website and the user, making it more difficult for attackers to intercept sensitive information.
5. **Two-factor authentication (2FA):** Two-factor authentication adds an extra layer of security to website logins by requiring users to enter a unique code in addition to their password. This can help prevent unauthorized access to the website.
6. **Employee training:** One of the most important resources for website security is a well-trained workforce. Providing employees with training on best practices for website security can help prevent attacks and minimize the impact of any breaches.

## Conclusion

Website Security is of utmost importance to all who maintain an online existence, whether it is a website for a hobby, a business, or a government entity. Protection against website attacks begins with understanding why they occur and taking action to protect the site. Whether it is an IN.gov-hosted site, one developed by agency personnel, or by a third party, good cyber awareness and adherence to best practices will protect the integrity of websites and those who view them.