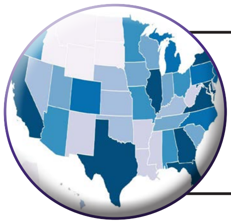
CyberWAtch

2017

OFFICE OF CYBERSECURITY HIGHLIGHTS FOR 2017: New cyber threats, the hunt for more security professionals, stats on attacks, advice on how to keep your data safe and more ...

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Index

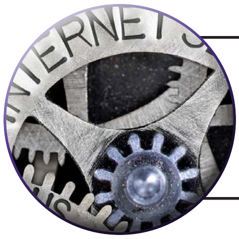


Office of CyberSecurity

Our mission:

Ensure continuity of commerce and continuity of government in the event of a cyber attack.

erWAtch



Protect individual privacy by safeguarding personal information of Washington state residents digitally stored by state government.

Engage regional national, public and private organizations to build stronger capabilities against cyber threats.

Provide leadership and establish strategic direction to ensure a statewide approach to cyber security.

The Big Picture

The cybersecurity landscape is changing rapidly, and not in a good way.

Cyberattacks are no longer the sole domain of nation states and a relatively small number of criminals with technical skills. Hackers now sell their services on the internet; much like private stores sell goods and services to the broader public online.

State and local governments, including Washington state, are seeing a surge in cyberattacks because of this and other factors, including the proliferation of devices being connected to the internet.

The exponential growth of attacks represents a challenge for both the public and private sector not only in terms of keeping pace with threat, but also in finding enough qualified cybersecurity professionals to defend networks.

Agnes Kirk, Washington State CISO

The Washington state Legislature and Governor's office created the Washington State Office of CyberSecurity (OCS) in July 2015 to guard

Cybersecurity.wa.gov

the state's networks against attacks.

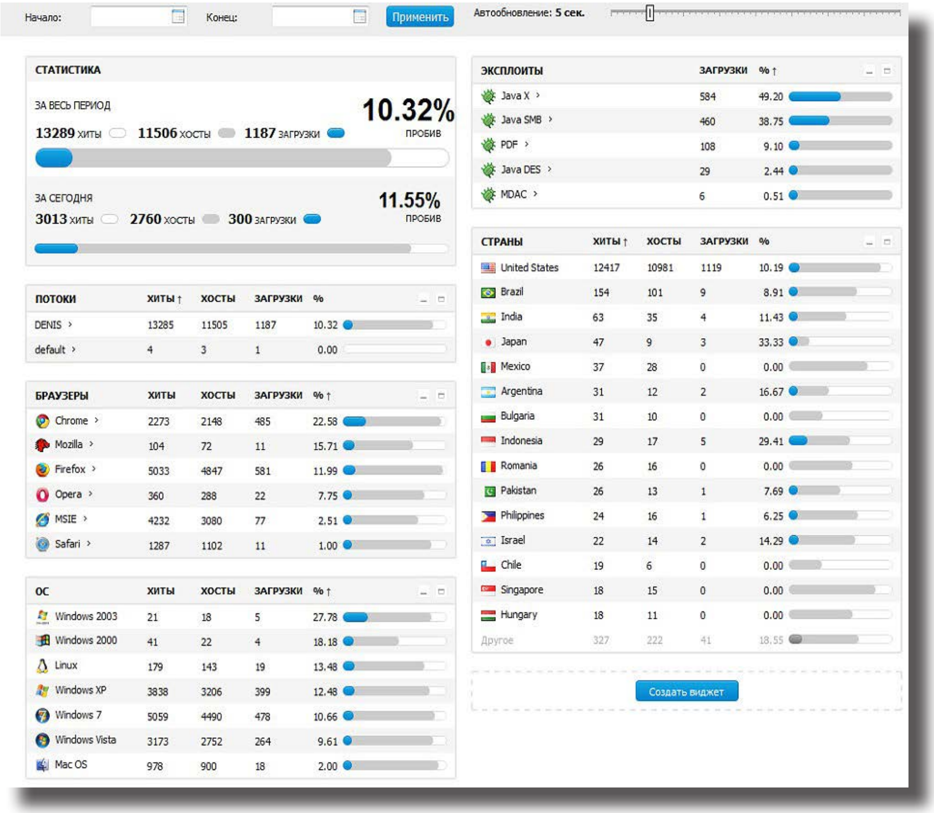
The office's cybersecurity team works 24 hours a day to detect, block and respond to cyberattacks. The office helps prevent and mitigate threats before they can cause significant damage.

In the past year alone, OCS blocked several billion unauthorized attempts to access the state's network and more than 80 million potentially malicious emails. OCS also successfully mitigated 15 major DDoS attacks in 2017 that were aimed at shutting down the state network.

In addition, our office works with state, local government and military agencies to build more secure networks. OCS sends out teams on a moment's notice to help state agencies with cyber threats.

As part of an ongoing outreach effort, our staff travels the state, speaking at colleges, libraries and retirement centers to provide information on how to stay safe online.

The office also runs an annual "Hacktober" cybersecurity quiz in October to raise state employee awareness as part of the National Cyber Security Awareness Month. The campaign, which tests state workers on their cyber knowledge, garnered more than 18,000 responses this year.



Начало: Конец: Применить Автообновление: **5 сек.**

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 ХИТЫ **11506** ХОСТЫ **1187** ЗАГРУЗКИ **10.32%** ПРОБИВ

ЗА СЕГОДНЯ

3013 ХИТЫ **2760** ХОСТЫ **300** ЗАГРУЗКИ **11.55%** ПРОБИВ

ПОТОКИ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS ›	13285	11505	1187	10.32
default ›	4	3	1	0.00

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome ›	2273	2148	485	22.58
Mozilla ›	104	72	11	15.71
Firefox ›	5033	4847	581	11.99
Opera ›	360	288	22	7.75
MSIE ›	4232	3080	77	2.51
Safari ›	1287	1102	11	1.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78
Windows 2000	41	22	4	18.18
Linux	179	143	19	13.48
Windows XP	3838	3206	399	12.48
Windows 7	5059	4490	478	10.66
Windows Vista	3173	2752	264	9.61
Mac OS	978	900	18	2.00

ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
Java X ›	584	49.20
Java SMB ›	460	38.75
PDF ›	108	9.10
Java DES ›	29	2.44
MDAC ›	6	0.51

СТРАНЫ	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00
Другое	327	222	41	18.55

Example of web site on the dark web where hackers sold their services much like any other business on the internet. (Source: krebsonsecurity.com)

We have more plans in the works, including:

Red Team: Will proactively test the security of the state's networks and services to help identify and fix potential vulnerabilities before a cyber attack can exploit and disrupt networks.

Application Certification and Accreditation Program: Will train application developers at government agencies on secure coding best practices and application of security patches.

Information Sharing and Analysis Center: Will collect, analyze and disseminate actionable threat information to public organizations and federal partners.

Cybersecurity.wa.gov

Threat Report

Cyb

Cybersecurity.wa.gov

During the past year, Washington state government has seen a significant increase in cyber threats including unauthorized attempts to access agency computers and distributed denial of service, DDoS, attacks aimed at shutting down the state network.

However, impersonation attacks — commonly referred to as phishing — continue to be the top reported event to for the state Office of CyberSecurity, OCS.

Spear phishing refers to specially crafted emails that hackers use to impersonate people known by the targeted users. Cyber criminals will mine public information, such as employee directories, to glean personal information they use in the emails to gain the trust of their victims.

Their aim: trick people into clicking on a link to provide login credentials, or download malicious software such as ransomware.

Only about 20 percent of all email sent to the state is allowed to its destination. The remainder is blocked because it's either malware or spam email. Many of the phishing messages OCS blocks contain links to temporary web sites used by hackers to harvest account credentials.

Government is a favorite target because agency databases contain a wealth of sensitive personal information hackers want to steal.

Phishing emails to government workers will often pretend to be from someone the employees know, or report to, such as an agency director or a supervisor, often referred to as spear phishing.

More general phishing emails will often pose as official correspondence from a bank, a government agency, such as the Internal Revenue Service, or stores where people frequently conduct business.

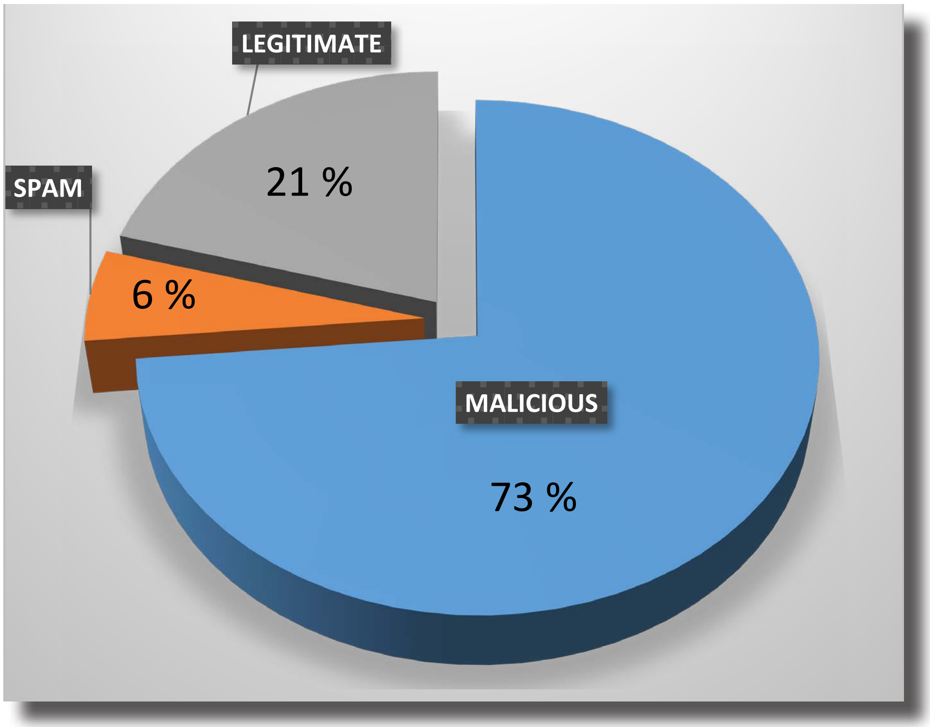
During past year, the U.S. saw a large spike in data breaches where spear phishing campaigns succeeded in tricking government agencies into providing employee W-2 forms.

The private sector also is experiencing a surge in these types of attacks. Eighty four percent of companies surveyed by Vanson Bourne in the U.S. and the United Kingdom last year reported that a spear phishing attack had made it through their security. The average impact of a successful attack: $1.6 million.

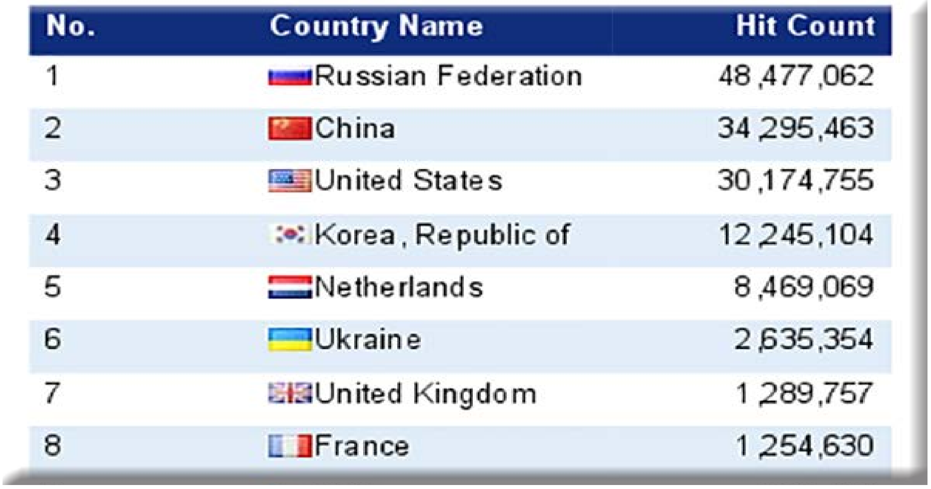
Many experts are concerned that some of the massive, private sector data breaches of personal information could lead to even more sophisticated attacks in the future because criminals now have access to a trove of detailed information.

Please see our tips to avoid becoming a phishing victim on page 12.

State Email Recieved, Distribution by Type



Top Cyber Attacks by Country: Jul - Dec



No.	Country Name	Hit Count
1	Russian Federation	48,477,062
2	China	34,295,463
3	United States	30,174,755
4	Korea, Republic of	12,245,104
5	Netherlands	8,469,069
6	Ukraine	2,635,354
7	United Kingdom	1,289,757
8	France	1,254,630

This chart shows number of attacks from IP addresses by country. The location of the IP address does not mean the attack originated in that country. Bad actors will often try to mask their location by routing attacks through servers in other countries.

Cybersecurity.wa.gov

Cyber Jobs

Cybersecurity.wa.gov

Corrinne Sande, center, is director of the Computer Sciences and Information Systems/CyberWatch West at Whatcom Community College, one of six programs in Washington state designated as a National Center of Academic Excellence in Information Assurance/Cyber Defense.

Like many of its peers, the State of Washington has a growing need for a skilled workforce in cybersecurity.

Providing government services often requires the collection of sensitive information. This data is stored on networks that require constant protection from online threats.

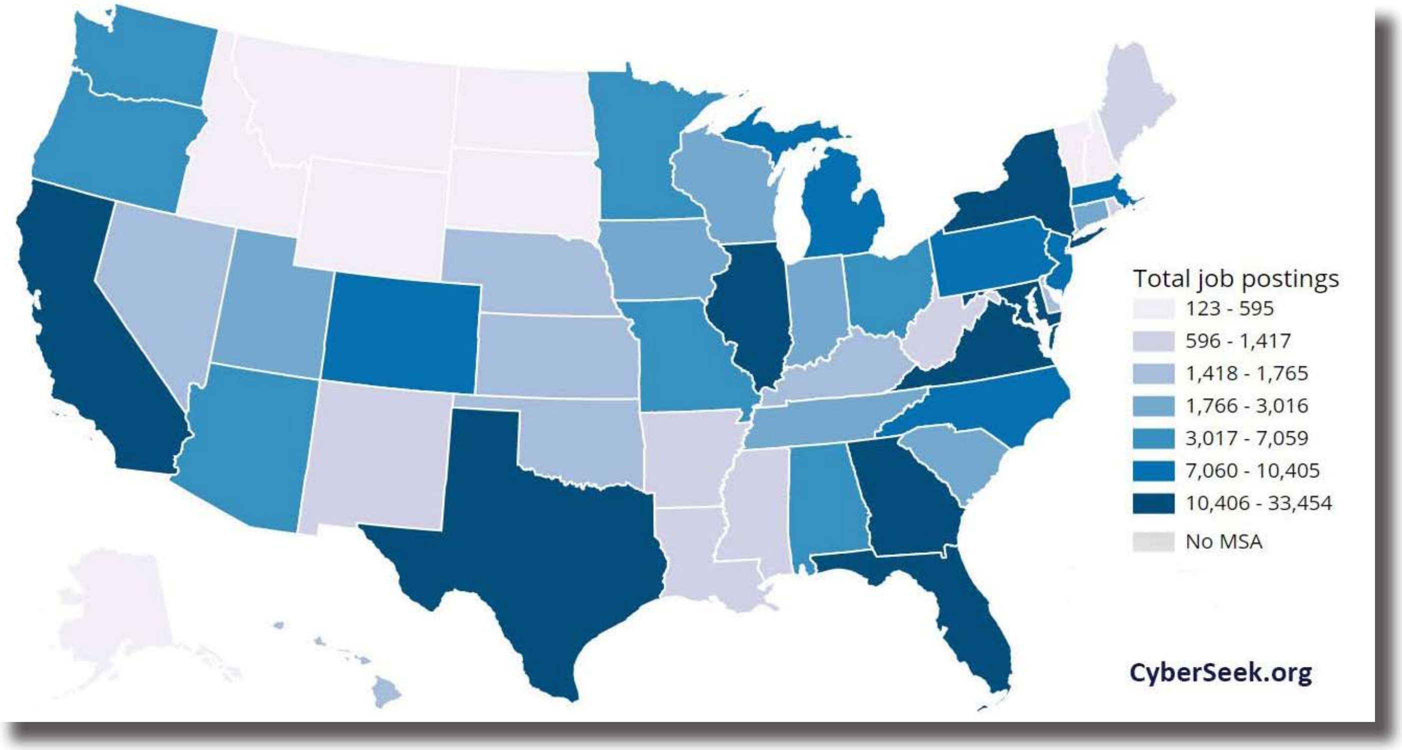
A severe shortage of cyber professionals in the labor market places this data and government services at risk.

There are currently more than 6,400 public and private sector cybersecurity job openings in Washington state and nearly 300,000 openings for cyber professionals nation wide.

The state of Washington and the state's Office of CyberSecurity (OCS) recognize the critical need to increase the pipeline of skilled and ready-to-hire applicants in the cyber security workforce.

To do this requires thinking about filling these jobs differently. We must create multiple paths to fill this workforce gap.

Whether you are a young person ready to pick a major in college, a veteran transitioning out of the military, or an early or mid-career worker wanting to make a career change into the cyber field, there should be erWAtch



There are more than 6,400 cybersecurity job openings in Washington state and nearly 300,000 cyber openings nation wide.

a way to get you there.

OCS, in collaboration with the business community and higher education, is working to help fill the void.

In 2017, our office worked with US Bank to bring in cybersecurity scholarships at the University of Washington in Seattle and Whatcom Community College in Bellingham. Our office also has a college internship program, not only to encourage more young people to seek careers in cybersecurity, but also to consider working for government agencies.

In addition, OCS is working with higher eductation programs and the National Security Agency, NSA, to develop an online curriculum that will allow more people to get the skills needed to fill these important jobs. Washington is lucky to have several nationally regarded cyber programs to help. The NSA has designated six Washington state colleges and universities as National Centers of Academic Excellence in Information Assurance/Cyber Defense.

It’s a distinguished designation that reflects the state’s commitment to developing cyber warriors and leaders. They are: Whatcom Community College in Bellingham, City University in Seattle, the University of Washington in Bothell, Highline College in Des Moines, Edmonds Community College, and Columbia Basin College.

Cybersecurity.wa.gov

Data Brokers

Cybersecurity.wa.gov

Have you ever recieved coupons in the mail for items you just bought at a store? Or received catalogs from companies you briefly visited online? Or had online ads for certain products follow you across the internet?

These aren't random coincidences.

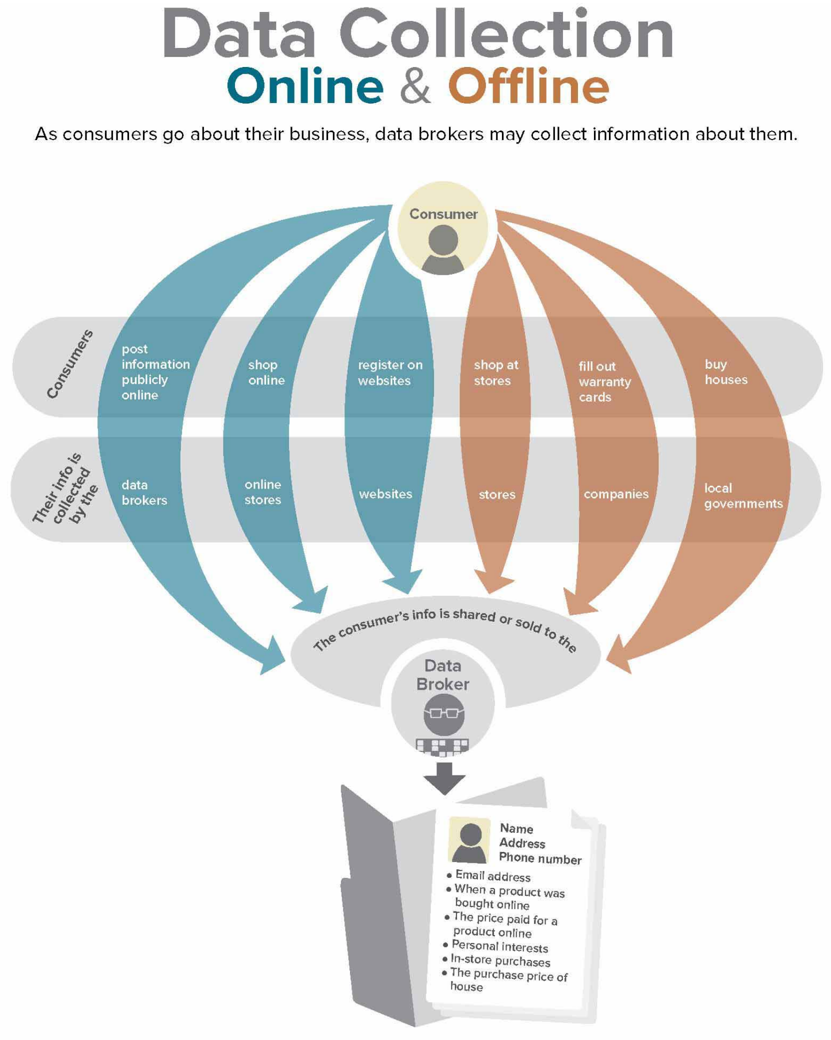
Companies you've likely never heard of monitor your financial transactions, analyze what you do on the internet, aggregate information from online forms you've filled out and use all that data to create detailed profiles.

They're called data brokers, and they sell all this information to the folks who send you those coupons, catalogs and place ads in your internet browser.

While many people don't mind this type of individualized marketing, there are other uses for the information that raise questions.

For example, concerns have been raised about data broker information potentially being used to set insurance premiums and determine loans, or even jobs.

A Federal Trade Commission report on data brokers *(Data Brokers: A Call for Transparency and Accountability)* stated marketers could use "seemingly innocuous inferences about consumers in ways that raise concerns. For example, while


Data Collection
Online & Offline
As consumers go about their business, data brokers may collect information about them.
Consumer
Consumers
post information publicly online
shop online
register on websites
shop at stores
fill out warranty cards
buy houses
Their info is collected by the
data brokers
online stores
websites
stores
companies
local governments
The consumer's info is shared or sold to the
Data Broker
Name
Address
Phone number
• Email address
• When a product was bought online
• The price paid for a product online
• Personal interests
• In-store purchases
• The purchase price of house

Federal Trade Commission

a data broker could infer that a consumer belongs in a data segment for 'Biker Enthusiasts,' which would allow a motorcycle dealership to offer the consumer coupons, an insurance company using that same segment might infer that the consumer engages in risky behavior."

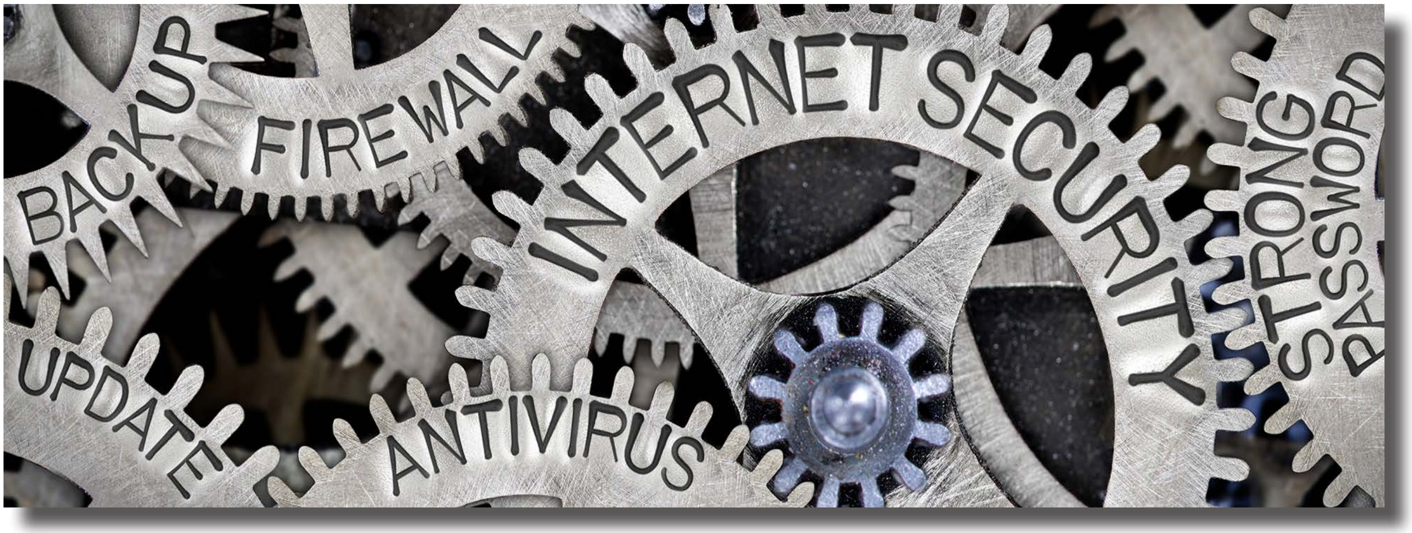
Information collected by data brokers also could "be used to facilitate harassment, or even stalking, and may expose domestic violence victims, law enforcement officers, prosecutors, public officials, or other individuals to retaliation or other harm," according to the report.

Short of living in a bunker with no connection to the outside world, there's no easy way to eliminate data brokers from collecting information about you. But there are steps you can take to help safeguard your privacy:

- Be careful about what you post on social media. For example, don't discuss medical conditions because that information could potentially be shared.
- Any time you sign up for a free service or app, be aware that the price of admission is often your data. If you don't want your information shared, consider whether you really need the app or service.
- If you want to surf the internet without being followed by data brokers, disable third-party cookies or use a browser extension that blocks tracking. Also, regularly clear your browser of cookies.
- Many data-brokers allow you to "opt-out" of their databases. You have to fill out forms at each data broker. The World Privacy Forum (worldprivacyforum.org) keeps an updated list of tips on how to opt out. Keep in mind that data brokers are constantly collecting information. So, for example, if you move, your records will reappear in databases.

Cybersecurity.wa.gov

Phishing Tips



Cybersecurity.wa.gov

Most data breaches start with a phishing email that tricks someone inside an organization into downloading malware, or providing their login credentials.

But it's getting a lot harder to distinguish legitimate messages from malicious ones that will let hackers gain control of your accounts.

Also, hackers are becoming increasingly sophisticated in their techniques, such as creating fake web pages that are nearly impossible to distinguish from the actual company or government agency site.

Here are some steps you can take to help protect yourself, and your organization, from becoming a victim:

- Don't trust email links or attachments. Hackers like to compromise the email accounts of people you trust and then send you email from those accounts, asking you to take certain actions, such as reading an attachment or going to a link.
- Telltale signs of a potential phishing email include messages from companies you don't have accounts with, spelling mistakes, and unexpected messages urging you to respond quickly, such as "Unpaid Invoice."
- If a company or organization sends you a link or phone number, don't click. Instead, look up the web page yourself in a search engine and use that address instead. The same rule applies to phone numbers. Do not use the phone numbers provided in an email. It could go straight to a hacker.
- Turn on two-factor authentication. This requires both your password and an additional piece of information to log in to your account. The second piece could be a code sent to your phone, or a random number generated by a smartphone app. This protects your account even if your password is compromised.
- Report suspicious emails to security staff. You can also forward phishing emails to spam@uce.gov – and to the organization impersonated in the email.

Cyber Hygiene

There are some things in life we do without thinking: washing our hands, morning showers, cleaning dishes. It's basic hygiene taught from an early age and carried through life.

As recent data breaches have demonstrated, cyber hygiene has become just as important.

Here are some recommended steps:

- Use one credit card for all online purchases: Credit cards are safer than debit cards for online purchases. The Fair Credit Billing Act protects credit card use, and using one card limits the potential for financial fraud to affect all of your accounts.
- Don't use the same login and password for all your accounts. Use several words strung together, such as easy to remember phrases, for passwords.
- Look for "https" in the internet address (URL) when making an online purchase. The "s" in "https" stands for "secure" and shows that communication with the webpage is encrypted.
- Do not use public computers or public wireless internet access for your online shopping. They can contain viruses and other malware that steal your information, which can lead to identity theft and financial fraud.
- Be careful about posting personal information on social media. Spear phishers will use it to pose as someone you trust in an email. They also may use the information to attempt breaking into your accounts.
- Keep your antivirus software up to date, as well as all other applications on your computer. Home users should have the auto update feature enabled. This will help protect against the latest threats.

Cybersecurity.wa.gov

Incident Checklist

State agencies must contact the state Office of CyberSecurity if there is a security incident, per OCIO Policy 143.

Here are key steps to follow during an incident:

□ Determine the problem & potential scope

□ Gather information

□ Determine what logs are available, in what detail & how far back?

□ Form an incident response team

□ Gather the team in a central location

□ Focus on containment

□ Document ALL changes

□ Assess how to recover

□ Formalize recovery schedule with roles, resources identified

□ Provide a detailed after action analysis

For Emergency Cyber Incident Reporting, call 360-407-8800. A security analyst will be reached immediately, 24x7, for significant cyber events

Cybersecurity.wa.gov

About Us

The Washington State Legislature created the Office of CyberSecurity (OCS) in 2015 to provide strategic direction for cybersecurity and protect state networks from growing cyber threats.

Here’s a quick overview of OCS services for state agencies:

Security Operations Center: The SOC is the state’s nerve center for cybersecurity monitoring and information sharing. It protects the state’s infrastructure from cyber threats by constantly monitoring state networks to detect, prevent and respond to cyber-attacks.

Computer Emergency Readiness Team: During a cyber security event, the CERT provides skilled experts to help state government agencies quickly respond to the incident, minimizing impact. The team handles all aspects of incident response from assessing the scope of an attack through recovery. The CERT also provides preventative service of a comprehensive cyber security risk assessment to help State of Washington agencies make informed decisions, lowering their possibility of an incident occurring.

Information Sharing and Analysis Center: This team shares intelligence gathered from law enforcement, third parties and OCS network monitoring with public and private sector partners to increase understanding and awareness of cyber threats.

Security Policy and Compliance: This team helps agencies reduce risk by developing standards and policies that represent best practices in architecture, network design, and application integrity. The SPC also helps ensure agencies follow the state-approved security architecture and security policies by reviewing the design of systems before they are put in place.

Contact information:

- **Visit us:** 1500 Jefferson St. SE, Olympia WA 98501
- **Email us:** cybersecurity@ocs.wa.gov
- **Call us:** (360) 407–8700 or 1–888–241–7597

Cybersecurity.wa.gov

OFFICE OF
CyberSecurity
STATE OF WASHINGTON

This document us available in alternative formats to accomdate persons with disabilities. Copies can be obtained by calling 360-407-9100.