ISSUE 27 WINTER 2020

RJ2 TECHNOLOGIES

Newsletter

What's Inside

Phishing attack exposes personal information of 5,000 at community college

St. Louis Community College, a four-campus system with more than 50,000 students, announced mid-February that a successful phishing campaign last month compromised the personal information of more than 5,000 students and employees.

The college issued a notice that "a series of email phishing attacks" discovered on Jan. 13 resulted in the exposure of names, student ID numbers, dates of birth, addresses, home phone numbers, cell phone numbers, and college and personal email addresses for 5,127 people. Of those affected, 71 also had their Social Security numbers compromised.

"There was a phishing email sent," said Nez Savala, the college's communications manager. "About 20-some people fell for it and that gave whoever was on the other end access to information that was stored in their email which led to access to student and employee information."

Those who clicked on the phishing links will be retrained on how to identify suspicious emails, a training session that all staff currently undergo annually, Savala said. Additionally, she said, all staff will be trained within the next 30 days on how to handle and share sensitive information.

Unfortunately for the college, the attacks came as it implementing multi-factor authentication for its email platform, a measure that may have prevented exposure of personal information. That functionality, however, was not launched until Jan. 31, Savala said.

To respond to the incident, the school notified those affected by email and traditional mail, set up a call center to field questions and offered free credit monitoring to those whose Social Security information has been exposed.

To explain the delay between identifying the incident on Jan. 13 and its public notice on Feb. 4, the college explained that first "several action steps needed to be taken."

"For example, information needed to be collected and analyzed from multiple systems to identify all of the impacted individuals and ensure the accuracy of the information that was contained in employee email accounts," the notice states.

The college reports it's notified the Department of Education's Office of Inspector General and the Family Policy Compliance Office and that it will continue to investigate the incident.

Phishing emails are a common attack vector in K-12 and higher education institutions. A similar scam, called a business email compromise, resulted last month in the theft of $2.3 million at a K-12 district in Texas.

Call RJ2 today to see what solutions you can provide to you, to keep your company safe from phishing atacks!

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

What is Bloatware, and how can you remove it?

Bloatware is software that nobody asked for but is on your computer, taking up valuable space. These software apps come with your hardware pre-installed, and very often, it isn't always apparent how to delete them properly.

SUPERFISH

In mid-2014, Lenovo users noticed that something was awry with their web browsers: banner ads were breaking webpage layouts and pop-ups were making surfing unpleasant. A deep dive into the problem led to the discovery of pre-installed software called Superfish — malware in the form of an adware pusher.

The app caused an uproar not only because of its disruptive ads, but also because it was found that Lenovo had essentially interrupted what's known in the industry as the certificate chain — a chain of trust whereby companies that run machines that users visit as they traverse the internet provide certificates that prove they're a legitimate party. With Superfish, Lenovo allegedly used self-signed certificates — as Lenovo is a known and trusted brand — making Superfish the root Certificate Authority (CA), meaning it can decide which encrypted communications to trust.

BLOATWARE EVERYWHERE

Microsoft has developed and deployed its fair share of bloatware as well. The Windows 10 operating system, in particular, has plenty of them, such as:

- Quicktime
- CCleaner
- uTorrent
- Shockwave Player
- Microsoft Silverlight
- Browser toolbars
- Coupon printer for Windows
- WinRAR
- Apps by the hardware manufacturer (laptop brand)

Some of these even run in the background and slow down computers without users knowing it.

While some users find value in these add-ons, many prefer to start with a leaner operating system due to storage space and processing power concerns. If they want a particular software, they prefer to download it themselves so they can have greater control over their machines and how they experience their hardware and software.

Like Superfish, other Windows 10 bloatware can also cause critical vulnerabilities. One ironic incident involved a pre-installed version of Keeper Password Manager. Instead of keeping passwords safe, it allowed malicious actors behind any website to steal passwords due to bloatware. While Windows 10 users needed to enable Keeper to store their passwords that exposed them to vulnerabilities, it makes you wonder why such a flawed password manager app was there in the first place.

HOW TO RID YOUR PC OF BLOATWARE

Removing inclusions you did not ask can be a hassle, but it's actually fairly easy. Windows has been kind enough to include a robust bloatware removal tool so that you can remove all apps you don't need. Here's how:

1. Click the Start menu and type Windows Security in the search bar.
2. Go to the Device Performance & Health section.
3. Scroll down and you'll see a section with the header "Fresh start". Click on the additional info link at the bottom.
4. Click on Get Started and accept the user account control (UAC) prompt.
5. The Fresh start interface should pop open. Click Next.
6. The tool will present a list of Windows 10 bloatware that will be removed
7. Review the list and click Next.
8. Click on Start.

Bloatware not only clutters your laptops and PCs, but it can also render your business vulnerable to cybersecurity breaches. Save yourself from tons of headaches down the line; learn more about protecting your computers from bloatware. Call our team of IT experts today.

FEATURED PARTNER

datto

Datto

Datto Inc. is an award-winning vendor of backup, disaster recovery (BDR) and Intelligent Business Continuity (IBC) solutions, providing best-in-class technology and support to its 5,000+ channel Partners throughout North America and Europe.

RJ2 SPOTLIGHT

Kevin Dann

Dispatch and IT Support Engineer

Kevin Dann has been in the professional field since 2012. After graduating from Purdue University, he started his career in the telecommunications field working as a project designer for Fullerton Engineering. Kevin joined RJ2 as an intern from 2010-2012 working onsite with qualifying engineers for projects. In 2019 he became a full-time employee at RJ2 as a Dispatch and IT Support Engineer.

Fun Fact: Kevin once meet Zachary Levi downtown Chicago.

BUSINESS PRESENCE

Here's how to speed up Google Chrome

Google made its foray into web browsers with Chrome in 2008. With its remarkable speed and ease, Chrome was welcomed by many users. However, over time, the browser becomes a bit sluggish, especially if you've installed extras such as extensions. Follow these easy steps to ramp up your Chrome browser's speed.

CLEAR YOUR BROWSING DATA

Chrome stores cached copies of websites you visit so it can load the page faster when you visit them again. It also keeps a database of your browsing history and cookies for the same purpose. As you visit more and more websites, these pieces of data accumulate in Chrome and can slow the browser down.

Thankfully, the solution is easy: clear your cache. Simply access your browsing history by entering chrome://history in your address bar. From the left panel, select Clear browsing data. Choose which data to delete by clicking on the checkboxes of all items you want deleted, like cached images or cookies. You can also select the time range that will be affected by the deletion. You can delete your history for the past hour, the last 24 hours, the last seven days, and from the beginning of time. Once you've selected the files you want to delete and their corresponding time range, click Clear data.

DISABLE EXTENSIONS

Extensions are downloadable programs from the Chrome Web Store that you can add to your browser to give it more functionality and a personalized touch. For example, you can add an extension that blocks ads, one that shortens URLs, or one that shows your most important tasks of the day. While these extensions are useful, they can slow Chrome down if there are too many installed at once.

Most extensions will show on Chrome's address bar, and you can quickly uninstall them by right-clicking on their icons and selecting Remove from Chrome. You can also manage all extensions by typing chrome://extensions in your browser and hitting Enter. From there, you'll find a list of all the extensions you have (even those you don't remember installing). Simply scroll through the list and click Remove to delete the extensions you don't need.

REMOVE ADS AND MALWARE

Sometimes, Chrome slows down because of malware or adware extensions. Extra toolbars, recurring pop-up ads, and web pages redirecting to other addresses are clear indications of these. Google once had a downloadable app developed for Chrome that scans and removes unwanted programs called the Clean Up Tool. In 2018, Google discontinued that app and made malware scanning even easier. Just type chrome://settings/cleanup in your browser, and click on Find to detect and remove harmful software on your computer.

A top-performing web browser benefits your business in many ways, including enhancing your employees' productivity and speeding up communication. If your web browser is performing poorly or takes forever to load a page, don't hesitate to get in touch with us so we can identify and fix the problem right away.

Feature Partner Product: SIRIS - Datto Product

Built for MSPs to ensure their customer's business is always on and resilient to disasters, SIRIS is an all-in-one solution that includes verified backups, restore options for any scenario, instant virtualization, and ransomware protection. All backed by Datto's private cloud.

Reliability begins with knowing your backup is always good. Datto eliminates the need to worry if the system will boot or be recoverable by building better backups that break free of incrementals and allow you to verify the backup is good before disaster strikes.

Even in the best scenario, downtime is incredibly costly for a business. With the ability to immediately get back up and running from the Datto Cloud, business owners maintain an edge over the local competition that can't bounce back as quickly.

March

"The new electronic independence re-creates the world in the image of a global village. "
- Marshall McLuhan

TECH TIPS OF THE MONTH

Below are some fun computer shortcuts!

1. **Stylizing text - Bold with CTRL+B, italicize with CTRL+I, and underline with CTRL+U**
2. **Editing text - Select all with CTRL+A, copy with CTRL+C, paste with CTRL+V**
3. **Made a mistake - Undo with CTRL+Z, redo with CTRL+B**
4. **Need a new page - Create a new page with CTRL+N**
5. **Saving - Save your work with CTRL+S**