


June 21, 2022

Challenge yourself with our Phishing quiz!

This past week's stories:

 **Credit unions across Canada targeted in cybersecurity incident, but no evidence data compromised: tech company**

£18m cyber-security hub centre opens at Abertay University

UK cybersecurity professionals overworked and lacking confidence to stop cyberattacks according to new survey

New malware on Google Play with over two million downloads

State-sponsored phishing attack targeted Israeli military officials

U.S., partners dismantle Russian hacking 'botnet,' Justice Dept says

Internet Explorer now retired but still an attacker target

Microsoft 365 credentials targeted in new fake voicemail campaign

Former Amazon employee convicted in Capital One hack

Cyber attackers spent median of 15 days inside victim networks last year: Sophos

From text messages to fraudulent ads, how scammers are draining bank accounts

CIRA Canadian Shield adds new browser extension to simplify online safety for Canadians

Credit unions across Canada targeted in cybersecurity incident, but no evidence data compromised: tech company

An unspecified number of credit unions in Manitoba and across Canada were hit by a targeted cybersecurity incident last week, and a company that provides digital technology services to credit unions says it has implemented a crisis response plan.

Celero Solutions, a Calgary-based company, says it became aware of "unauthorized access to the company's systems" on June 8.

<https://www.cbc.ca/news/canada/manitoba/credit-unions-cybersecurity-incident-1.6488872>

Click above link to read more.

[Back to top](#)

£18m cyber-security hub centre opens at Abertay University

A new £18m cyber-security research centre has been officially opened at Abertay University in Dundee.

The cyberQuarter centre, which is the first of its kind in Scotland, covers four floors for use by businesses, academics, and students.

<https://www.bbc.com/news/uk-scotland-tayside-central-61738018>

Click above link to read more.

[Back to top](#)

UK cybersecurity professionals overworked and lacking confidence to stop cyberattacks according to new survey

The demands placed on cybersecurity professionals struggling to cope with the risks faced by their organisations from cyberattack were evaluated in a new survey of 300 cybersecurity and IT workers in mid-sized organizations in the UK. The survey was commissioned by Arctic Wolf®, a leader in security operations. Over a quarter (27%) of survey respondents stated that they do not feel knowledgeable enough as an individual to spot a cyber threat. This, coupled with the fact that 30% of surveyed cybersecurity workers said that they do not know how to use their organisation's security tools effectively, suggests that UK organisations are in a precarious and insecure cybersecurity position.

<https://www.globenewswire.com/news-release/2022/06/15/2463554/0/en/UK-Cybersecurity-Professionals-Overworked-and-Lacking-Confidence-to-Stop-Cyberattacks-According-to-New-Survey.html>

Click above link to read more.

[Back to top](#)

New malware on Google Play with over two million downloads

As a result of the recent investigation into the Google Play Store, researchers discovered adware and malware that steals information from users. At least five of the apps were still available when they were discovered last month, and have more than two million downloads.

<https://cybersecuritynews.com/malware-on-google-play/>

Click above link to read more.

[Back to top](#)

State-sponsored phishing attack targeted Israeli military officials

An advanced persistent threat group, with ties to Iran, is believed behind a phishing campaign targeting high-profile government and military Israeli personnel, according to a report by Check Point Software.

Targets of the campaign included a senior leadership in the Israeli defense industry, the former U.S. Ambassador to Israel and the former Deputy Prime Minister of Israel.

<https://threatpost.com/phishing-attack-israeli-officials/179987/>

Click above link to read more.

[Back to top](#)

U.S., partners dismantle Russian hacking 'botnet,' Justice Dept says

Law enforcement in the United States, Germany, the Netherlands and Britain dismantled a global network of internet-connected devices that had been hacked by Russian cyber criminals and used for malicious purposes, the U.S. Justice Department said on Thursday.

The network, known as the "RSOCKS" botnet, comprised millions of hacked computers and devices worldwide, including "Internet of Things" gadgets like routers and smart garage openers, the department said in a statement.

<https://www.reuters.com/world/us-partners-dismantle-russian-hacking-botnet-justice-dept-says-2022-06-16/>

Click above link to read more.

[Back to top](#)

Internet Explorer now retired but still an attacker target

Microsoft's official end-of-support for the Internet Explorer 11 desktop application on June 15 relegated to history a browser that's been around for almost 27 years. Even so, IE still likely will provide a juicy target for attackers.

That's because some organizations are still using Internet Explorer (IE) despite Microsoft's long-known plans to deprecate the technology. Microsoft meanwhile has retained the MSHTML (aka Trident) IE browser engine as part of Windows 11 until 2029, allowing organizations to run in IE mode while they transition to the Microsoft Edge browser. In other words, IE isn't dead just yet, nor are threats to it.

<https://www.darkreading.com/vulnerabilities-threats/internet-explorer-will-likely-remain-an-attacker-target-for-some-time>

Click above link to read more.

[Back to top](#)

Microsoft 365 credentials targeted in new fake voicemail campaign

A new phishing campaign has been targeting U.S. organizations in the military, security software, manufacturing supply chain, healthcare and pharmaceutical sectors to steal Microsoft Office 365 and Outlook credentials.

The operation is ongoing and the threat actor behind it uses fake voicemail notifications to lure victims into opening a malicious HTML attachment.

<https://www.bleepingcomputer.com/news/security/microsoft-365-credentials-targeted-in-new-fake-voicemail-campaign/>

Click above link to read more.

[Back to top](#)

Former Amazon employee convicted in Capital One hack

A former Amazon Web Services employee was convicted of hacking into Capital One and stealing the data of more than 100 million people nearly three years ago in one of the largest data breaches in the United States.

Paige Thompson, who worked for the software giant as an engineer until 2016, was found guilty on Friday of seven federal crimes, including wire fraud, which carries up to 20 years in prison. The other charges, illegally accessing a protected computer and damaging a protected computer, are punishable by up to five years in prison. A jury found Thompson not guilty of aggravated identity theft and access device fraud after 10 hours of deliberations, a release said.

<https://www.cnn.com/2022/06/18/former-amazon-employee-convicted-in-capital-one-hack.html>

Click above link to read more.

[Back to top](#)

Cyber attackers spent median of 15 days inside victim networks last year: Sophos

Cyber attackers are spending longer time inside business systems after hacking them. According to a new report from cyber security firm, Sophos, the threat actors spent a median of 15 days inside victim networks last year, an increase of over 36% from the previous year.

This concept is called 'dwell time' – that is the length of time between assumed initial intrusion and detection of an intrusion. The usual assumption is that the shorter the dwell time, the less damage can be done, and hence its importance.

<https://www.livemint.com/technology/tech-news/cyber-attackers-spent-median-of-15-days-inside-victim-networks-last-year-sophos-11655718465441.html>

Click above link to read more.

[Back to top](#)

From text messages to fraudulent ads, how scammers are draining bank accounts

In the 25 years Helen Cahill has kept the books for her small business near Melbourne Airport, she's never had any trouble doing online banking.

So on a particularly busy afternoon on May 26, when she sat down at her desk, she thought it was strange it was taking so long to log in.

<https://www.abc.net.au/news/2022-06-21/scammers-using-text-messages-calls-emails-fake-ads-to-get-money/101167848>

Click above link to read more.

[Back to top](#)

CIRA Canadian Shield adds new browser extension to simplify online safety for Canadians

CIRA is proud to announce the launch of its highly requested desktop browser extension for CIRA Canadian Shield that makes it easier than ever for Canadians to protect themselves against growing online threats. This free-to-use browser extension—available on popular browsers such as Google Chrome and Mozilla Firefox—will help protect more Canadian internet users from harmful malware, phishing attempts, scams and other malicious actors.

Searching the web can turn into risky business for many individuals and families across the country, especially when bumping into the wrong site becomes a security trap and infects a laptop or an entire network. As 54 per cent of Canadians say they spend more than five hours online per day, doing it safely at home or on the road is still a major concern in most households.

<https://www.globenewswire.com/news-release/2022/06/21/2466099/0/en/CIRA-Canadian-Shield-adds-new-browser-extension-to-simplify-online-safety-for-Canadians.html>

Click above link to read more.

[Back to top](#)

Click [unsubscribe](#) to stop receiving the Digest.

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

<http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest>

To learn more about information security issues and best practices, visit us at:

<https://www.gov.bc.ca/informationsecurity>

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

