Sysoft.ca

SECURITY & AWARENESS TRAINING QUARTERLY NEWSLETTER

2024 Q4

What's New

We're thrilled to announce some exciting additions to our newsletter this quarter!

Dive into our expanded coverage of Canadian IT security news. Whether it's breaking news or in-depth analysis, our goal is to provide you with the most relevant and timely information for the perspective that matters, yours!

But that's not all! We're also including a fascinating section on the use of AI to create deepfakes. This poses a significant security risk to everyone. Discover the implications, and what you need to know to stay protected.

Help us help you by completing the security poll that has also been included! We believe the results will be fascinating so please participate.

WHAT'S INSIDE THIS ISSUE?

Canadian Security News

In this section, we bring you the latest updates and insights into the ever-evolving world of IT security in Canada. From emerging threats and innovative defense strategies to regulatory changes and expert opinions, our curated selection of articles will keep you informed and prepared. Dive into our featured stories and stay ahead of the curve in safeguarding your digital landscape by clicking on the links below.

Get Cyber Safe

Homepage of the Government of Canada Get Cyber Safe campaign. Find out where the risks are, how to protect yourself and how to protect your devices.

Get Cyber Safe / Oct 8

[Get Cyber Safe]

MFA Isn't Failing, But It's Not Succeeding: Why a Trusted Security Tool Still Falls Short

Multi-factor authentication is a necessary safeguard, but its limitations show why organizations can't rely on it alone to prevent breaches.

SecurityWeek / Oct 7

[MFA Isn't Failing, But It's Not Succeeding Why a Trusted Security Tool Still Falls Short]

October is Cyber Security Awareness Month in Canada

Cyber Security Awareness Month (Cyber Month) is an internationally recognized campaign held each October to help the public learn more about the importance of cyber security. The campaign helps Canadians...

Get Cyber Safe / Jul 22

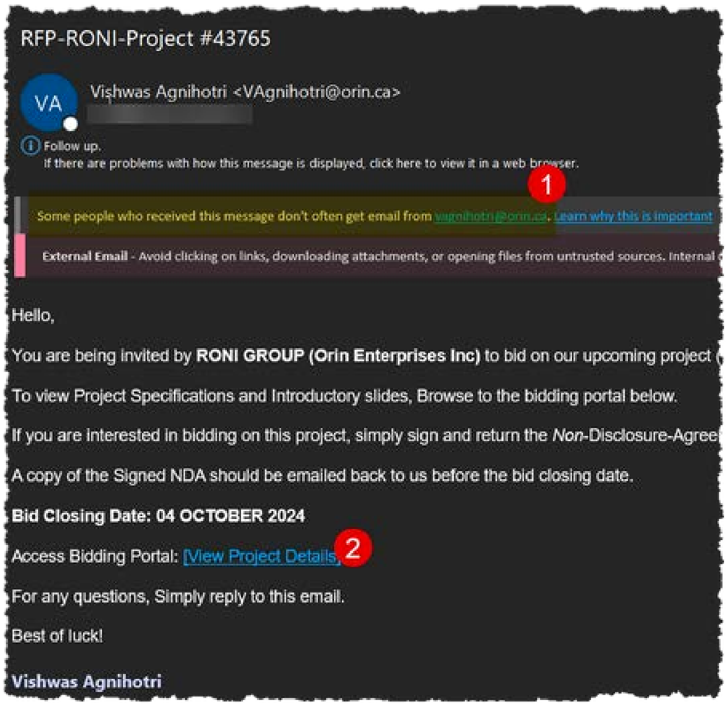
[October is Cyber Security Awareness Month Get Cyber Safe]

Trendiest Phish

It’s time again for another edition of the trendiest phish! Where we cover the topic of what’s hot in the cybercriminal world in which bad actors can use to steal your data. This newsletter’s topic is Implicit Trust.

Implicit Trust - “It’s ok because it’s you!”

Now you might ask, what is implicit trust? This type of trust makes users perform actions based on the assumption that everyone or everything is trustworthy from certain sources but not everywhere. For this newsletter, we’ll be focusing on how phishing emails are often overlooked due to implicit trust. This can lead to serious consequences. The screenshot to your right highlights an email from a security incident where implicit trust was assumed for one reason or another. In this example, an email from a company requesting an RFP (Request for Proposal) was received. As this was part of the user’s normal day to day activities, they ignored obvious red flags and made assumptions because they believed the email was from a trusted source leading to an account breach.



RFP-RONI-Project #43765

Vishwas Agnihotri <VAgnihotri@orin.ca>

[redacted]

Follow up.
If there are problems with how this message is displayed, click here to view it in a web browser.

1

Some people who received this message don’t often get email from vagnihotri@orin.ca. Learn why this is important

External Email - Avoid clicking on links, downloading attachments, or opening files from untrusted sources. Internal

Hello,

You are being invited by **RONI GROUP (Orin Enterprises Inc)** to bid on our upcoming project (

To view Project Specifications and Introductory slides, Browse to the bidding portal below.

If you are interested in bidding on this project, simply sign and return the *Non*-Disclosure-Agree

A copy of the Signed NDA should be emailed back to us before the bid closing date.

Bid Closing Date: 04 OCTOBER 2024

Access Bidding Portal: [View Project Details] 2

For any questions, Simply reply to this email.

Best of luck!

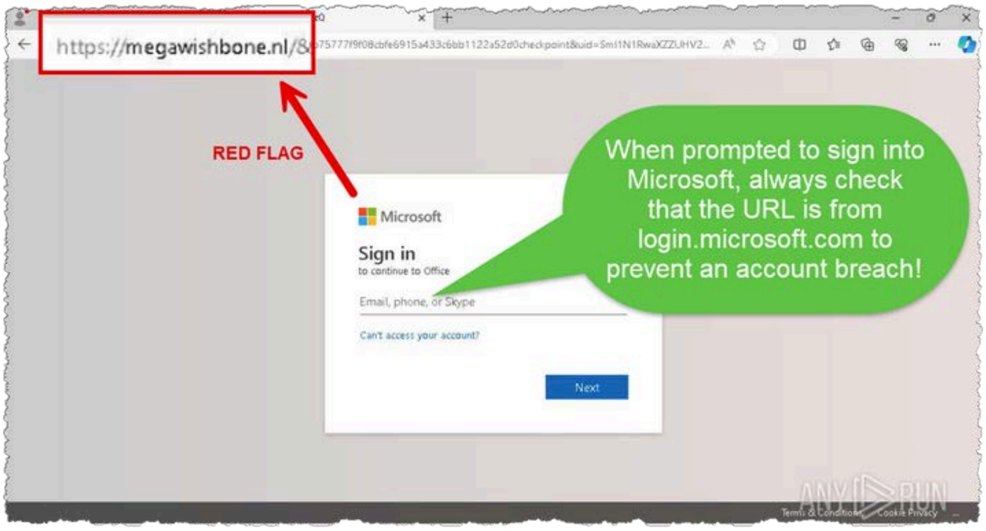
Vishwas Agnihotri

Trendiest Phish

The Red Flags

Here is a breakdown of the inconsistencies that Sysoft found in the email and throughout the phishing attack that led to the account breach:

1. An external email address was flagged because emails weren't often received from the sender.
2. A very suspicious link was included in the email that when moused over did not appear legitimate.
3. The link opened a suspicious website that looked very basic asking for another link to be clicked.
4. The new link opened another suspicious website located in the Netherlands requiring a checkbox to be clicked in order to proceed.
5. After the checkbox was clicked, a fake Microsoft sign-in website opened causing the user to enter their credentials including MFA.



https://megawishbone.nl/&575777f9f08cbfe6915a433c6bb1122a52d0checkpoint&uid=Sml1N1RwaXZZUHV2...

When prompted to sign into Microsoft, always check that the URL is from login.microsoft.com to prevent an account breach!

There are many different ways to identify suspicious messages. The following method may be the simplest and quickest approach that we can recommend. When you receive an email ask yourself these questions for each email:

- Do I know the sender?
- Was I expecting something from the sender?

If you answer no to question #1 then you should consider reporting the message if it appears to be malicious in any way. If you answer yes to question #1 but no to question #2 then you should probably give the sender a call to be safe before doing anything else! Keep yourself safe.

Deepfakes

Deepfakes**,** also known as audio fakes, face swapping or video cloning, are a type of generated media that can be very deceptive. Artificial intelligence (AI) is used to create highly realistic audio, or video that mimic real people. The term “deepfake” combines “deep learning” and “fake,” reflecting the technology’s reliance on deep learning techniques to generate these convincing forgeries.

Origins and Evolution of Deepfakes

- The concept of manipulating media isn’t new and can be traced back to the 1990s when researchers began exploring AI-generated content.
- The significant leap in the technology came with the invention of Generative Adversarial Networks (GANs) by Ian Goodfellow in 2014.
- The term “deepfake” emerged in 2017 when a Reddit user named “deepfakes” started sharing videos that used face-swapping technology.

Advancements in Deepfake Technology

- Over the years, deepfake technology has become increasingly sophisticated, producing media that is often indistinguishable from real footage.
- Tools for creating deepfakes have become more accessible, from software to apps that are freely available to the public.

How Deepfakes are Used in Phishing

- Audio Deepfakes
    - Attackers use AI to clone a person’s voice, impersonating trusted individuals to deceive victims into revealing sensitive information or transferring money.
    - An example of this could be when an employee receives a call from someone sounding exactly like their boss, instructing them to wire funds to a specific account.

- Video Deepfakes
    - Attackers create realistic videos of trusted individuals, such as company executives, to manipulate victims into taking specific actions.
    - An example of this could be when a video message from a supposed company executive is received asking an employee to share confidential information.

Deepfakes

Tips to Prevent Falling for Deepfakes

- Audio Deepfakes
    - Always verify the identity of the caller through a secondary method, such as a known phone number or in-person confirmation.
    - Be cautious of urgent or unusual requests, especially those involving financial transactions or sensitive information.
- Video Deepfakes
    - Look for unnatural facial movements, lip-sync issues, or unusual lighting that might indicate a video is fake.
    - Confirm the message through other trusted communication channels, such as email or in-person meetings.

By understanding the origins and advancements of deepfake technology, and implementing these preventive measures, you can better protect yourself from falling victim to deepfake phishing attacks.

Security Poll

Calling all guardians of cyber space! Take our security poll and help us defend you against digital threats!

In an age where every click, tap, or swipe could potentially lead to a security breach, it's crucial for us to band together and fortify our defenses against cyber threats. That's why we're inviting you to click the link below and participate in this quarter's set of questions:

https://forms.office.com/r/txB6y2t8s6

Whether you're a seasoned security professional, a vigilant online user, or somewhere in between, your perspective is invaluable in our mission to protect digital realms from malicious actors. Together, let's strengthen our collective resilience and take a stand against cyber threats. Complete our security poll today and join the frontline defenders of the digital world!

SAT Quarterly Newsletter Q4 Security Poll

Team Message

As part of our ongoing commitment to your security and awareness, we want to remind you of the importance of staying vigilant against phishing attacks. These deceptive attempts to steal your personal information are becoming increasingly sophisticated, but there are simple steps you can take to protect yourself when something does not feel right.

- Trust your instincts!
- Verify the source!
- Be skeptical of urgent requests!
- Check for red flags!
- Report suspicious activity!

Remember, your awareness and caution are our first line of defense against these constantly evolving types of threats. Stay informed, stay secure, and don't hesitate to reach out if you have any questions or concerns.

We hope you enjoy this quarter's newsletter! Stay tuned for more updates, as we continue to bring you valuable information and insights in each edition. Thank you for being a valued reader, and we look forward to sharing more with you in the future.

Thank you from your security and awareness training team.

Have any questions, or concerns? Get support with Sysoft.

Visit docs.sysoft.info/GETHELP for more information.