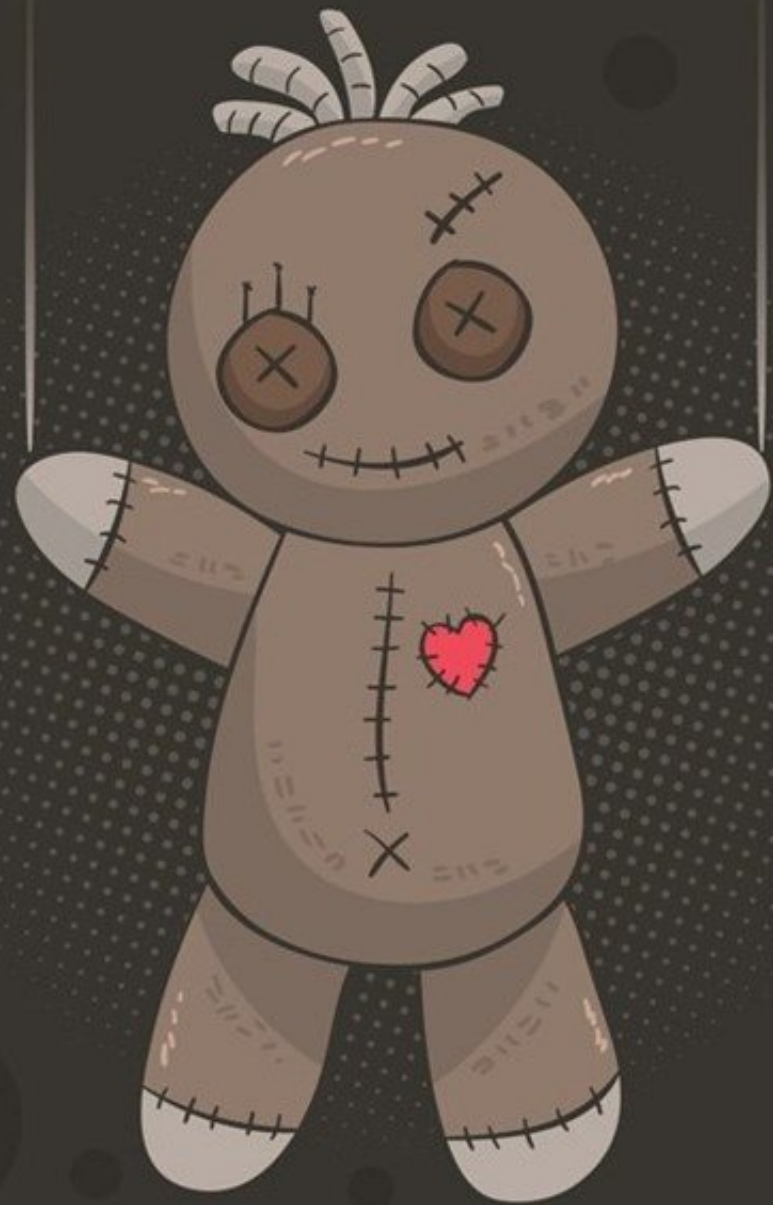


DON'T LET HACKERS
PULL YOUR STRINGS



Learn

S

M

A

R

T

Cyber Skills

*Holiday Hackers are busy at work.
Here are some tips to keeping your
business safe*



TurnKey Solutions

225-751-4444 www.turnkeysol.com

*Headlines like these are infiltrating your RSS Feed these days...
And with good reason, CyberSecurity has never been more
important than it is today!*



How to protect your business and its data during the 2021 holiday season

It's the first year of major holiday travel in the post-pandemic remote work world. Here's what businesses can do to protect themselves from elevated holiday cybersecurity risks.

Brandon Vigliarolo - December 9, 2021, 10:18 AM PST



Just in time for Christmas, Kronos payroll and HR cloud software goes offline due to ransomware

The attack has led to an outage expected to last weeks, leaving companies scrambling to make payroll with the holidays right around the corner.

Brandon Vigliarolo - December 15, 2021, 7:36 AM PST

Baby Dies in Alabama Hospital Due to Ransomware, According to Lawsuit
By Scrubs October 1, 2021 A new lawsuit alleges that a baby born with severe brain injury at a hospital in Alabama died, at least in part, because the facility was suffering from a ransomware attack, which led to a botched medical procedure.

[Baby Dies in Alabama Hospital Due to Ransomware, According ...
scrubsmag.com/baby-dies-in-alabama-hospital-due-to-ransomware-according-to-la...](https://scrubsmag.com/baby-dies-in-alabama-hospital-due-to-ransomware-according-to-la...)

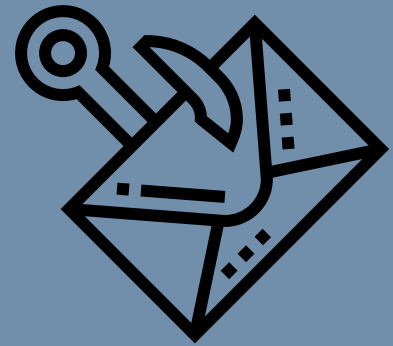
Smishing kicks into high gear as scammers use package delivery texts as clickbait

Proofpoint finds that bad actors are using SMS messages about package deliveries as the bait in new scams.

Veronica Combs - November 23, 2021, 2:00 AM PST



Think you know all the different types of hacks out there already?



Phishing



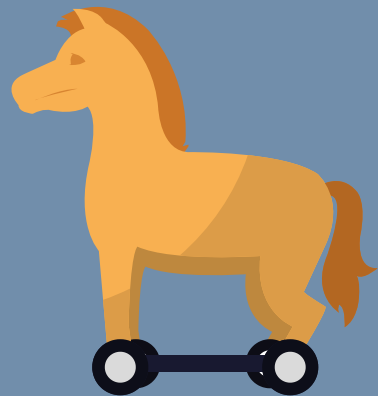
DNS Spoofing



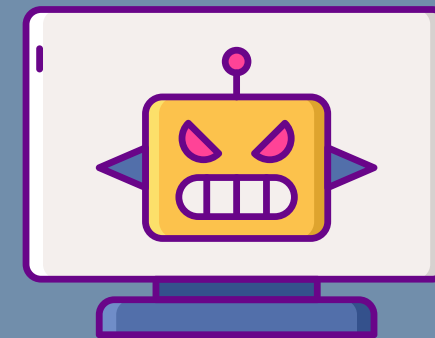
Smishing



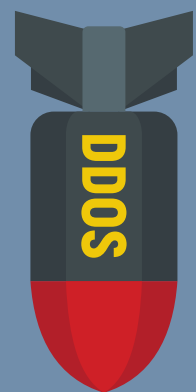
Fake Ads & Sites



Malware



Botnets



Denial of Service

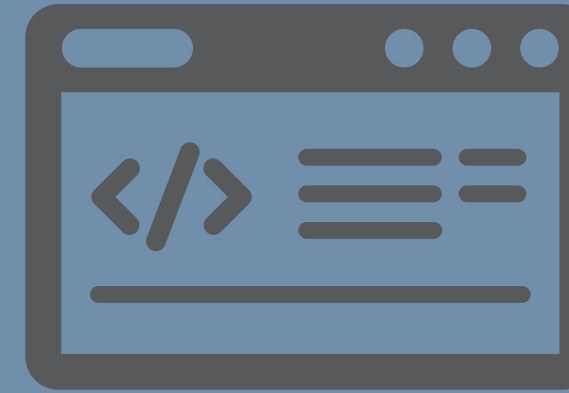


Credential Theft

And even more types of attacks...



Man in the Middle



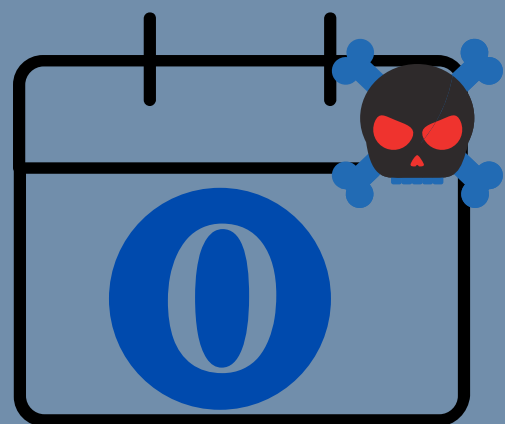
Cross-Site Scripting



SQL Injections



Click Bait Text



Zero Day Exploit









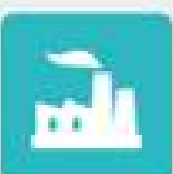


Drive-By Downloads

Know your risk:



Who's at Risk?

The top three industries by company size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
 44.7% Healthcare & Pharmaceuticals	 49.7% Construction	 55.9% Technology
 41.1% Education	 49.2% Healthcare & Pharmaceuticals	 49.3% Healthcare & Pharmaceuticals
 40.9% Manufacturing	 43.5% Business Services	 46.8% Manufacturing



Samples of how they try to fool you:

Secure Your WellsFargo Online Key - Message (HTML)

File Message Tell me what you want to do

Delete Archive Reply Reply Forward All Create New Move Mark Unread Categorize Follow Up Translate Zoom

Wells Fargo <inmail-hit-reply@linkedin.com> James Sat 10/22

Secure Your WellsFargo Online Key

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear James,

We are writing to inform you that the Personal Security Key your for your Wells Fargo Account has expired, as a result, is no longer valid.

This email has been sent to safeguard your Wells Fargo Account against any unauthorized activity. For your online account safety click the link below to reactivate your key:

http://cabinetkignima.com/Wellsfargo_keys_account5/page2.html

Wells Fargo Support

Reply Not interested

View Wells's LinkedIn profile

TIP You can respond to Wells by replying to this email

You are receiving InMail notification emails. [Unsubscribe](#)
This email was intended for James (). [Learn why we included this.](#)

If you need assistance or have questions, please contact [LinkedIn Customer Service](#).

© 2016, LinkedIn Corporation. 2029 Stierlin Ct Mountain View, CA 94043, USA

Windows Error Report - Message (HTML)

Microsoft Team <no-reply_microsoft@outlook.com>

Windows Error Report

Windows User Alert

Unusual sign-in activity

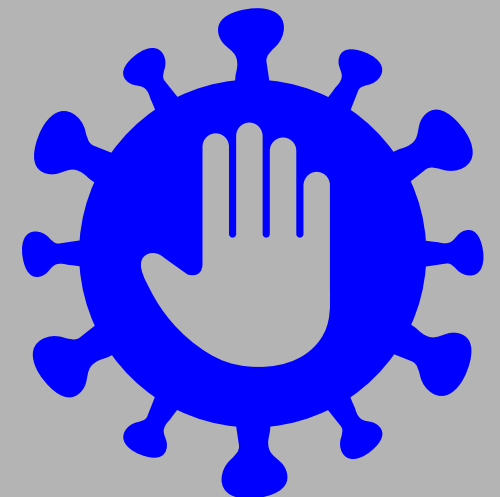
We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign IP Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

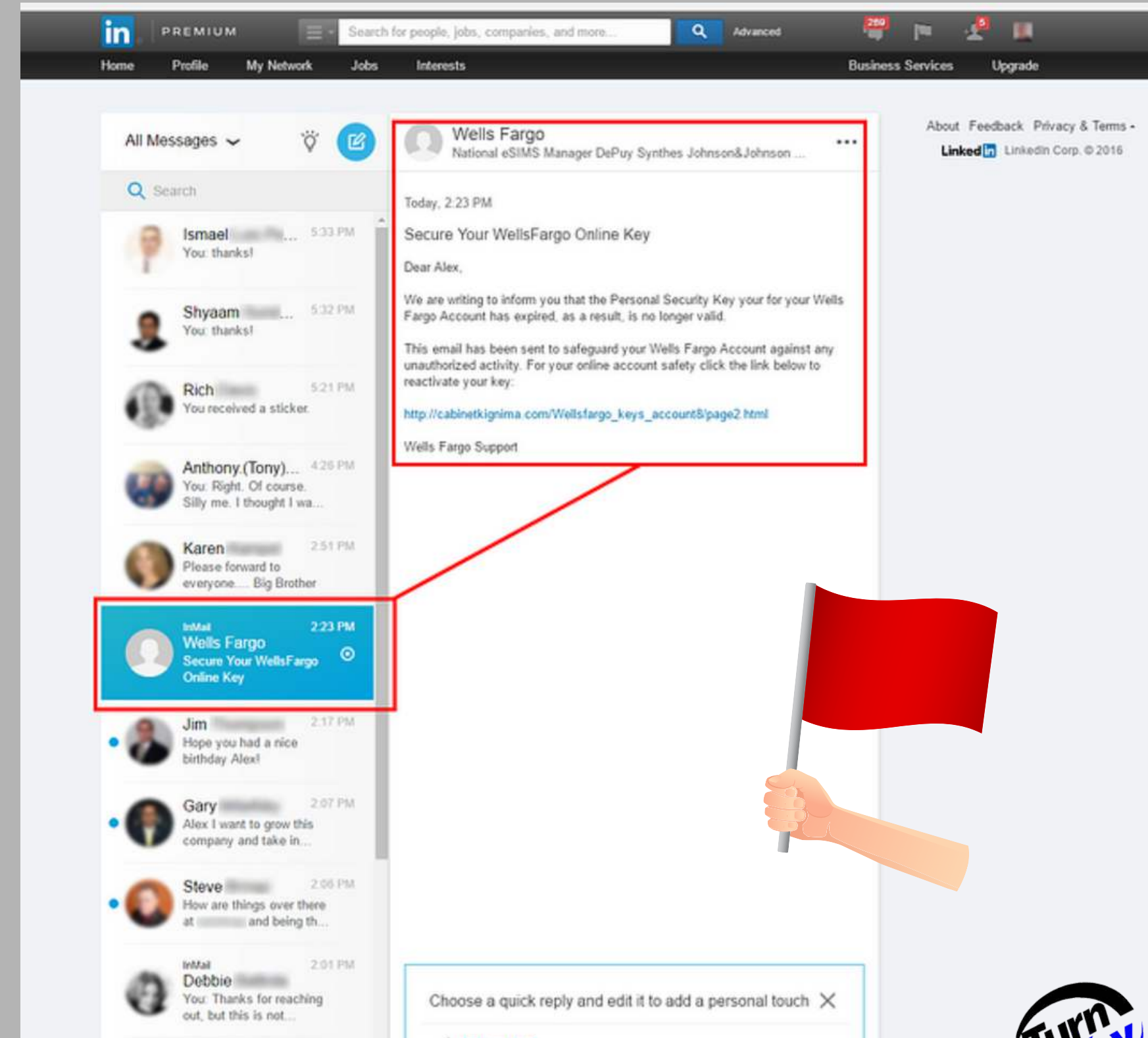
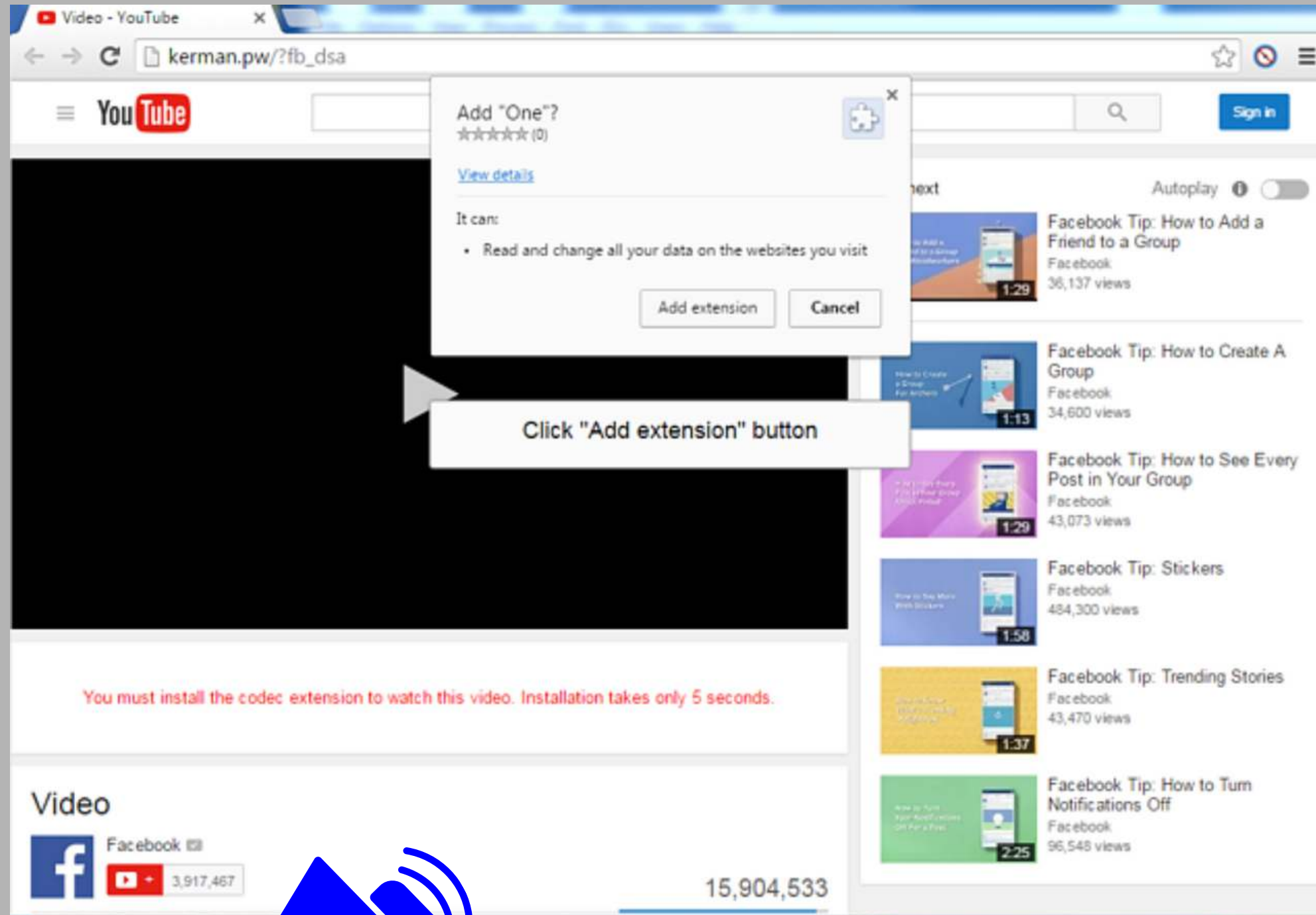
If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately 1-800-816-0360 or substitute you can also visit the Website: <https://www.microsoft.com/> and fill out the consumer complaint form. Once you call, please provide your Reference no: AZ-1190 in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

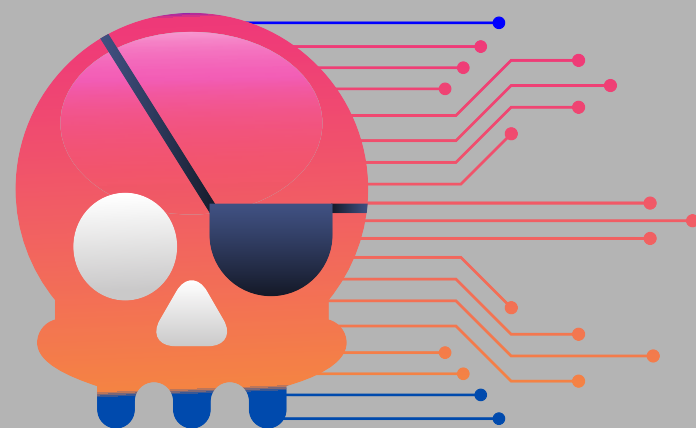
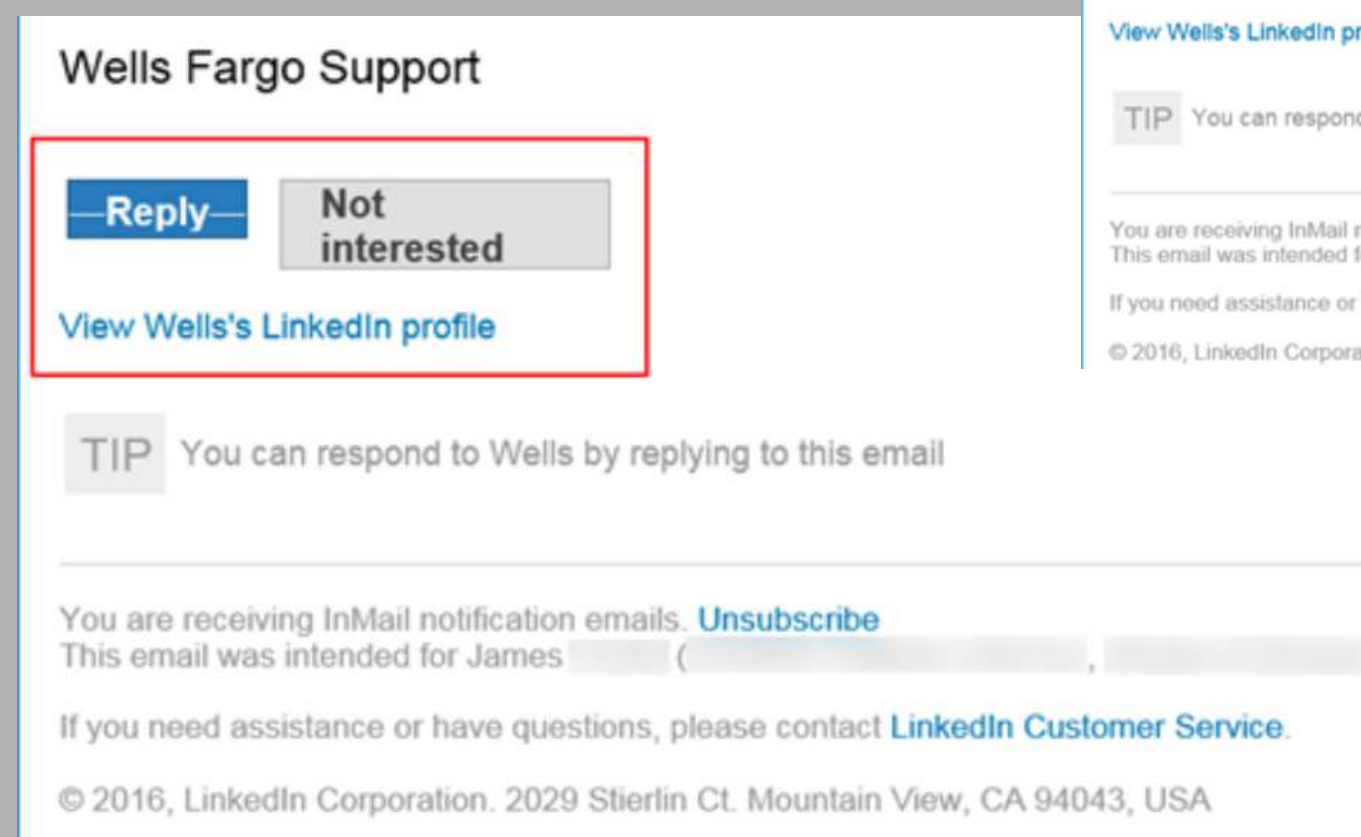
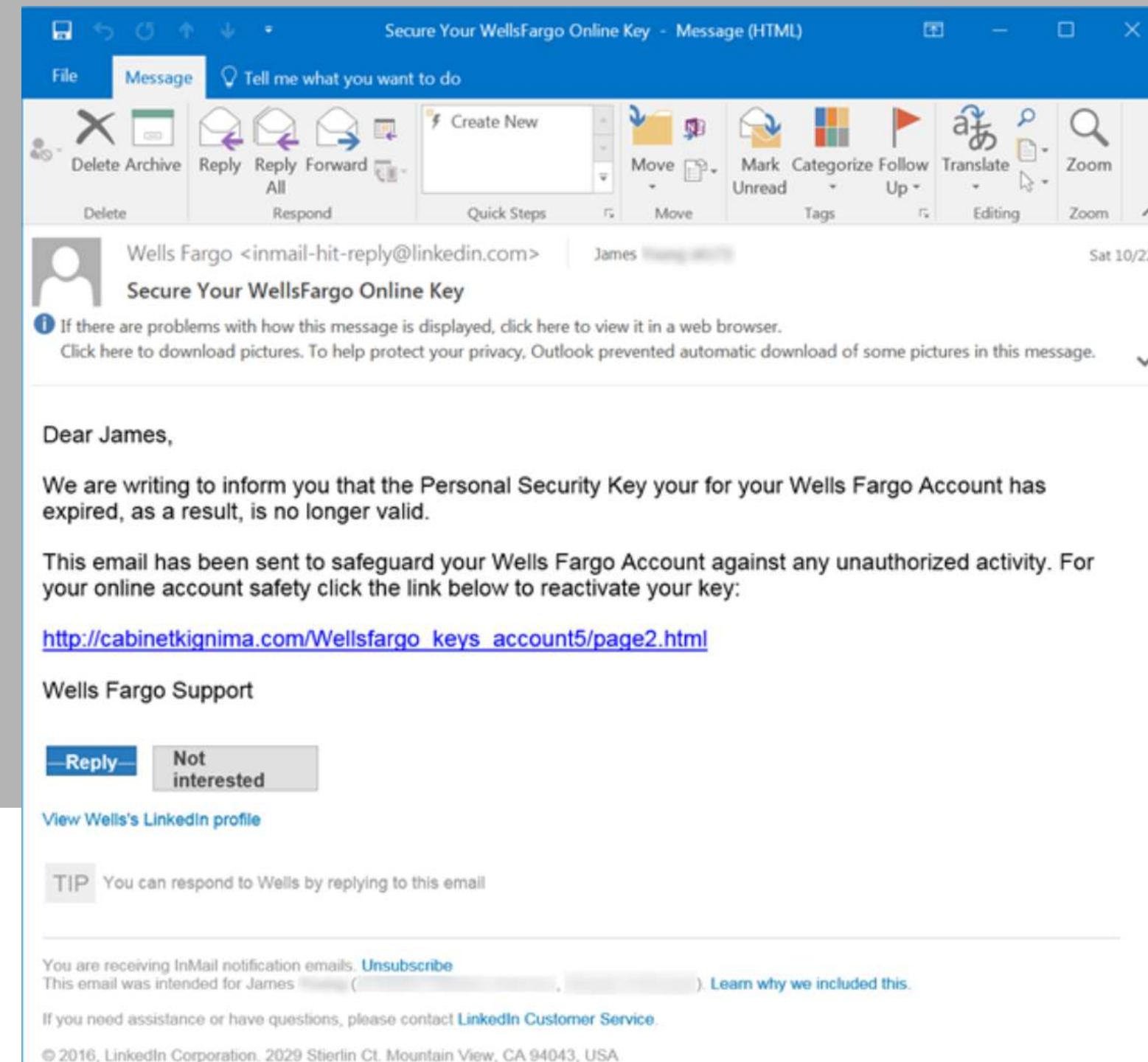
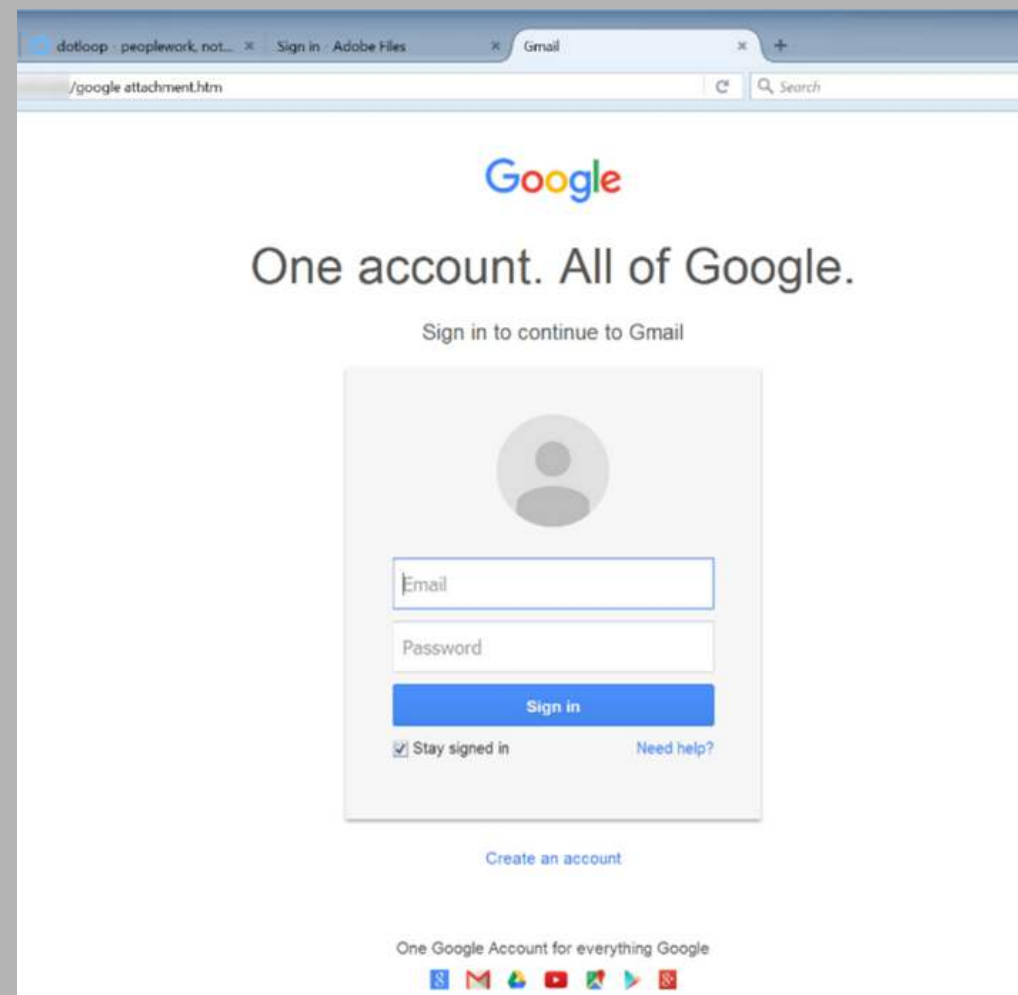
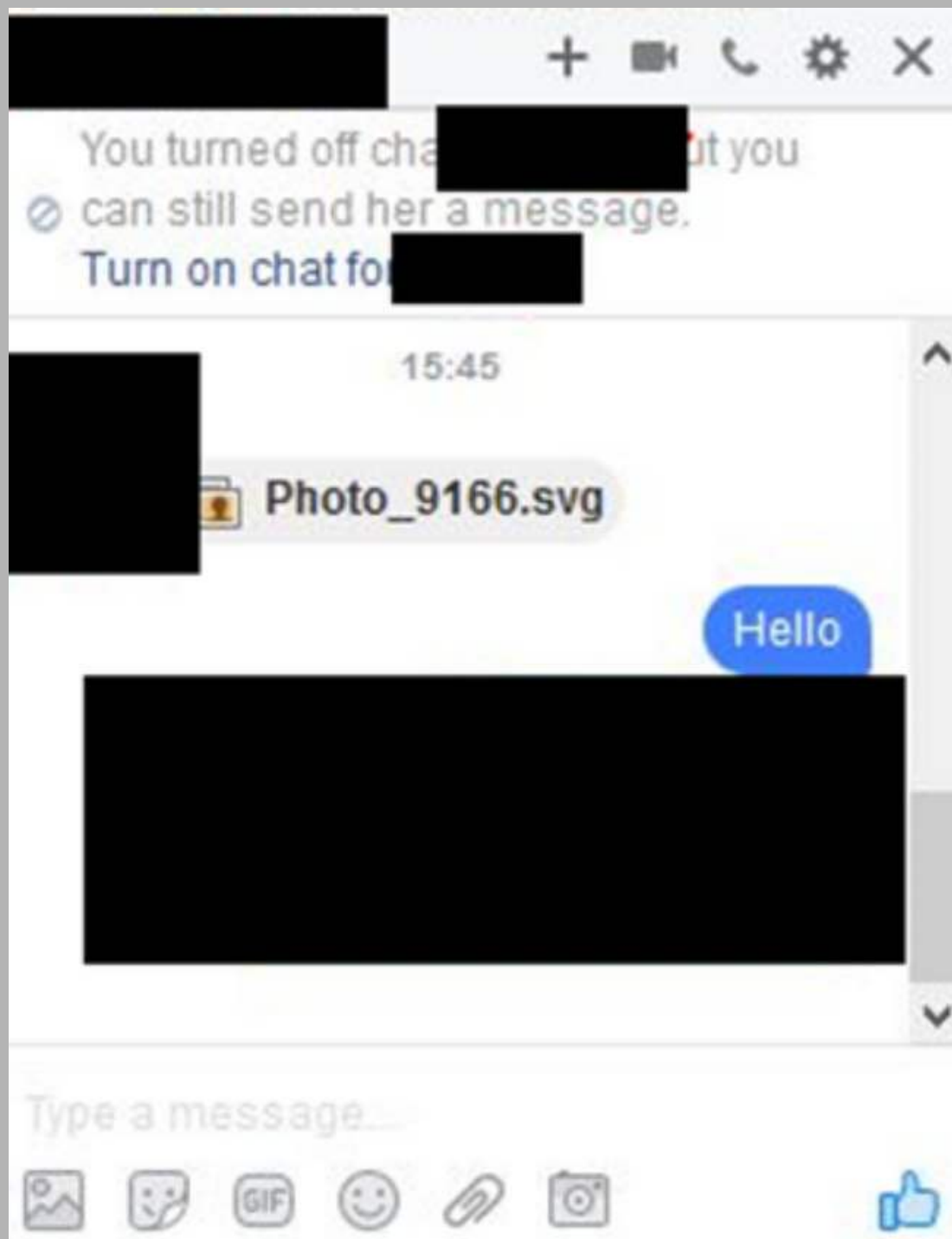
[Review recent activity](#)



Samples of how they try to fool you:



Samples of how they try to fool you:





Feeling Overwhelmed Now? Don't Give Up - We Are Here to Help!



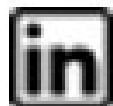
[Facebook.com/TKSLA](https://www.facebook.com/TKSLA)

Follow our Facebook page for 3-7 weekly updates, training resources & industry newsflashes, as well as helpful videos about a variety of security, business and productivity subjects.



[Twitter.com/tksllc](https://twitter.com/tksllc)

Join the conversation with us on Twitter (@TKSLLC) for important news updates & training resources



[Linkedin.com/company/turnkey-solutions-llc](https://www.linkedin.com/company/turnkey-solutions-llc)

Our LinkedIn community offers a great place to collaborate, stay updated, and find training resources, videos and more.



www.Turnkeysol.com

Browse our hundreds of blog articles about security, technology, business and productivity guides.



Email Tech Tips, Newsletter

We send out weekly *short and important* email regarding the latest in technology, security, and business productivity, and a monthly newsletter with I.T. news, recommendations and more!



[www.Youtube.com/user/hdlo2025](https://www.youtube.com/user/hdlo2025)

Browse our video library of tech talks & webinars about security, technology, business and productivity guides.



And MUCH MORE

We offer powerful, fully managed & reported Training & Testing resources on Security, HIPAA, NIST, and more.



Also check out our partners at KnowBe4 for some very helpful tools and resources:



Security Awareness Training Resources

Security awareness training resources including free tools, whitepapers, and more. Also get in-depth data about cybersecurity threats like phishing and ransomware.

[knowbe4.com](https://www.knowbe4.com)

www.knowbe4.com/resources

www.knowbe4.com/phishing

Free Tools

 Phishing Security Test Did you know that 91% of successful data breaches started with a spear phishing attack? Go Phishing Now!	 Phish Alert Button Do your users know what to do when they receive a suspicious email or attachment? Get Your Phish Alert Button	 Phishing Reply Test How many of your users will take the bait and reply to a spoofed email? Test Your Users
---	--	---

Free IT Security Tools

Test your users and your network with our free IT Security tools which help you to identify the problems of social engineering, spear phishing and ransomware attacks.

 Phishing Security Test Did you know that 91% of successful data breaches started with a spear phishing attack?	 Awareness Program Builder Get your free customized Automated Security Awareness Program with calendar and PDF.	 Phish Alert Button Do your users know what to do when they receive a suspicious email or attachment?	 Domain Spoof Test One of the first things hackers try is to see if they can spoof the email address of your CEO.
 Ransomware Simulator Tool Is your network effective in blocking ransomware and social engineering attacks?	 Weak Password Test Did you know 81% of hacking-related breaches used either stolen and/or weak passwords?	 Email Exposure Check Pro Have your users made you an easy target for spear phishing? Find out now!	 Domain Doppelgänger Find out if your domain has an evil twin with the Domain Doppelgänger tool.

www.knowbe4.com/free-it-security-tools



STILL HAVE QUESTIONS?

Reach out anytime:

ask@tksl.com

support@tksl.com

www.turnkeysol.com

225-751-4444



TurnKeySolutions