
Cyber Security and You
A guide to not giving your IT team more grey hairs

STATISTICS

It's estimated that 3.4 billion fraudulent emails are sent daily.

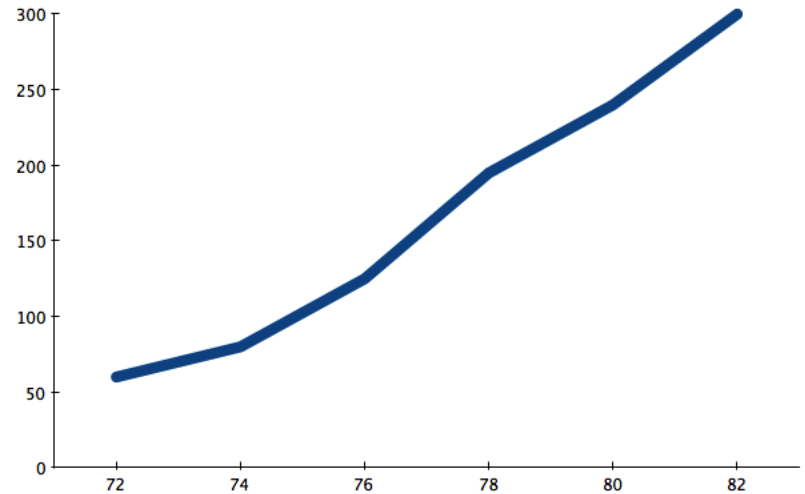
It's estimated that 3.4 billion fraudulent emails are sent daily.
6.9% of all phishing related websites are Logistics/Shipping

It's estimated that 3.4 billion fraudulent emails are sent daily.
6.9% of all phishing related websites are Logistics/Shipping
94% of all cyber attacks are carried out through emails

It's estimated that 3.4 billion fraudulent emails are sent daily.
6.9% of all phishing related websites are Logistics/Shipping
94% of all cyber attacks are carried out through emails
Phishing emails account for 90% of all data breaches

It's estimated that 3.4 billion fraudulent emails are sent daily.
6.9% of all phishing related websites are Logistics/Shipping
94% of all cyber attacks are carried out through emails
Phishing emails account for 90% of all data breaches
Highest cause of successful phishing attacks is human error

It's estimated that 3.4 billion fraudulent emails are sent daily.
6.9% of all phishing related websites are Logistics/Shipping
94% of all cyber attacks are carried out through emails
Phishing emails account for 90% of all data breaches
Highest cause of successful phishing attacks is human error



*scary looking generic graph showing continual growth for current topic

EXAMPLES

From: Michael Butterfield <kikismith910@gmail.com>
Sent: Friday, August 12, 2022 10:31 AM
To: Coral Snell <csnell@frontierscs.com>
Subject: QUICK ONE

Hi Coral,

I am leaving for a meeting now, and I want to know if you can complete a task for me ASAP ?

Please give me your personal phone number.

Thanks,

Michael Butterfield.

Sent from my iPhone

From: Michael Butterfield <kikismith910@gmail.com>
Sent: Friday, August 12, 2022 10:31 AM
To: Coral Snell <csnell@frontierscs.com>
Subject: QUICK ONE

Hi Coral,

I am leaving for a meeting now, and I want to know if you can complete a task for me ASAP ?

Please give me your personal phone number.

Thanks,

Michael Butterfield.

Sent from my iPhone

From: jquirke@frontierscs.com <jquirke@frontierscs.com>
Sent: Friday, May 30, 2025 3:16 AM
To: John Quirke <jquirke@frontierscs.com>
Subject: ALERT! I'm hacked you and stolen you information
Importance: High

Hey jquirke@frontierscs.com,

I have to share bad news with you.

Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts **jquirke@frontierscs.com** .
Obviously, I have easily hack to log in to your email.

Your password: password sourced from another data breach published online

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to access your email.
In fact, it was not really hard at all (since you were following the links from your inbox emails).
All ingenious is simple. =)
This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).
I have downloaded all your information, data, photos, web browsing history to my servers.
I have access to all your messengers, social networks, emails, chat history and contacts list.
My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter...

From: jquirke@frontierscs.com <jquirke@frontierscs.com>
Sent: Friday, May 30, 2025 3:16 AM
To: John Quirke <jquirke@frontierscs.com>
Subject: ALERT! I'm hacked you and stolen you information
Importance: High

Hey jquirke@frontierscs.com,

I have to share bad news with you.

Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts **jquirke@frontierscs.com** .
Obviously, I have easily hack to log in to your email.

Your password: password sourced from another data breach published online

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to access your email.
In fact, it was not really hard at all (since you were following the links from your inbox emails).
All ingenious is simple. =)
This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).
I have downloaded all your information, data, photos, web browsing history to my servers.
I have access to all your messengers, social networks, emails, chat history and contacts list.
My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter...

From: jquirke@frontierscs.com <jquirke@frontierscs.com>
Sent: Friday, May 30, 2025 3:16 AM
To: John Quirke <jquirke@frontierscs.com>
Subject: ALERT! I'm hacked you and stolen you information
Importance: High

Hey jquirke@frontierscs.com,

I have to share bad news with you.

Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts **jquirke@frontierscs.com** .
Obviously, I have easily hack to log in to your email.

Your password: password sourced from another data breach published online

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to access your email.
In fact, it was not really hard at all (since you were following the links from your inbox emails).
All ingenious is simple. =)
This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).
I have downloaded all your information, data, photos, web browsing history to my servers.
I have access to all your messengers, social networks, emails, chat history and contacts list.
My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter...

From: jquirke@frontierscs.com <jquirke@frontierscs.com>
Sent: Friday, May 30, 2025 3:16 AM
To: John Quirke <jquirke@frontierscs.com>
Subject: ALERT! I'm hacked you and stolen you information
Importance: High

Hey jquirke@frontierscs.com,

I have to share bad news with you.

Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts **jquirke@frontierscs.com** .
Obviously, I have easily hack to log in to your email.

Your password: password sourced from another data breach published online <-

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to access your email.
In fact, it was not really hard at all (since you were following the links from your inbox emails).
All ingenious is simple. =)
This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).
I have downloaded all your information, data, photos, web browsing history to my servers.
I have access to all your messengers, social networks, emails, chat history and contacts list.
My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter...

From: Michael Butterfield <mbutterfield@frontierscs.com>
Sent: Wednesday, August 24, 2022 10:30 AM
To: Maureen Magura <mmagura@frontierscs.com>
Subject: AT OFFICE?

Maureen,

I would like you to handle an urgent outgoing payment, kindly respond as soon as this email reaches you.

Thanks
Michael Butterfield

Sent from my T-Mobile 4G LTE Device

https://help.frontierscs.com/helpdesk/tickets/5779

čt 12.11.2020 21:48

Admin-Notification@[redacted]

[redacted] Password Expiration Report : 11/12/2020

To [redacted]

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Office 365

ID: [redacted]

Your password for [redacted] is set to expire on Thursday, November 12, 2020.
You can change or continue with the same password with below button.

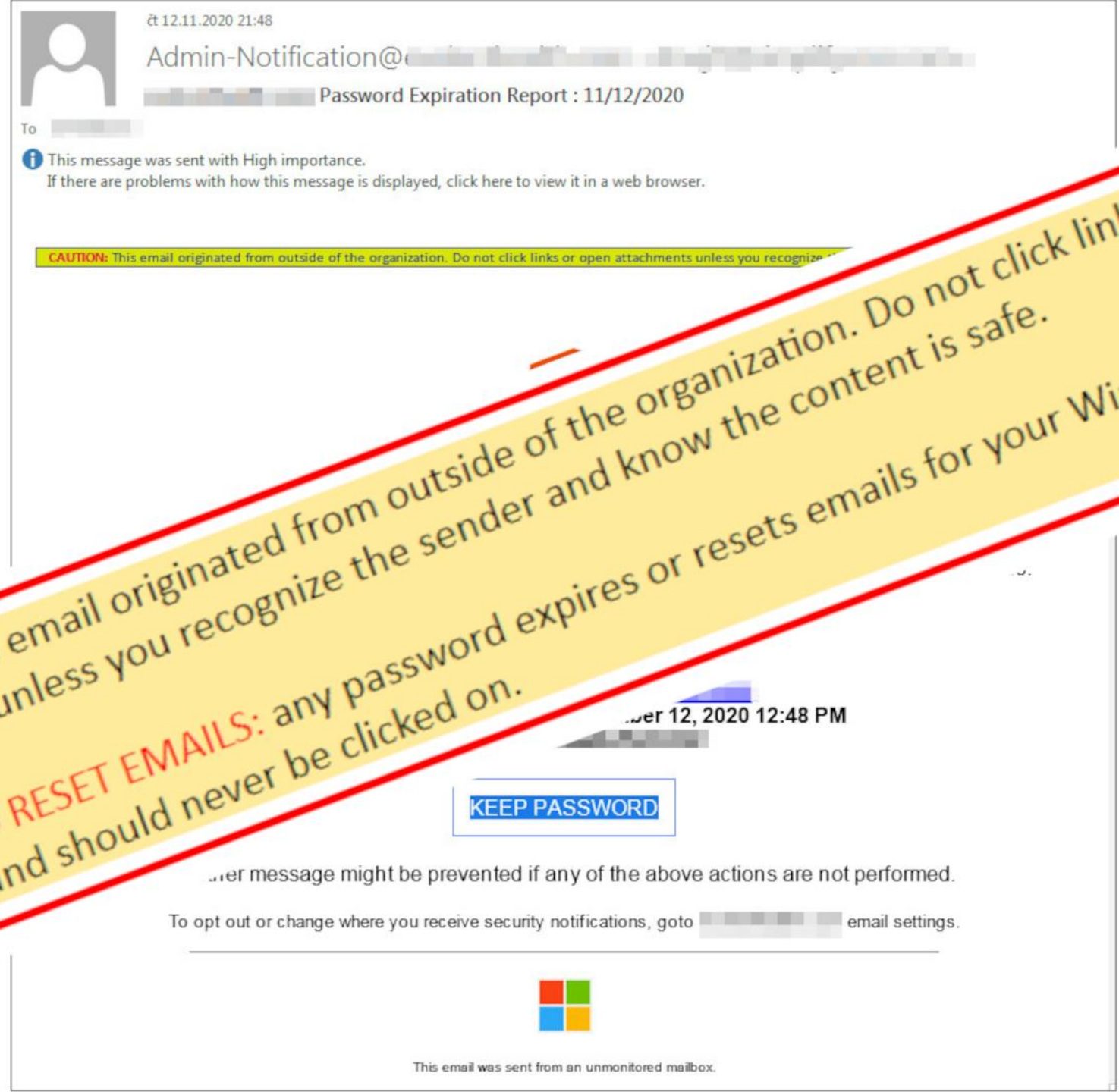
Email: [redacted]
Expiration Date: Thursday, November 12, 2020 12:48 PM
Error Code: [redacted]

KEEP PASSWORD

Further message might be prevented if any of the above actions are not performed.

To opt out or change where you receive security notifications, goto [redacted] email settings.

This email was sent from an unmonitored mailbox.



CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

PASSWORD RESET EMAILS: any password expires or resets emails for your Windows account are FAKE and should never be clicked on.

What Can You Do

When in doubt, submit it to support@frontierscs.com

(I couldn't think of a rhyme that works)

When in doubt, submit it to support@frontierscs.com

(I couldn't think of a rhyme that works)

If it looks suspicious but from a regular sender, call or send them a message to verify

When in doubt, submit it to support@frontierscs.com

(I couldn't think of a rhyme that works)

If it looks suspicious but from a regular sender, call or send them a message to verify

If you are unsure, ask

When in doubt, submit it to support@frontierscs.com

(I couldn't think of a rhyme that works)

If it looks suspicious but from a regular sender, call or send them a message to verify

If you are unsure, ask

Always make sure the email address matches the sender

When in doubt, submit it to support@frontierscs.com

(I couldn't think of a rhyme that works)

If it looks suspicious but from a regular sender, call or send them a message to verify

If you are unsure, ask

Always make sure the email address matches the sender

If you are unsure, ask