Protecting Your Computer and Your Privacy

© *Ruth E. Thaler-Carter*
TechWrite-SL, January 2020

The issue

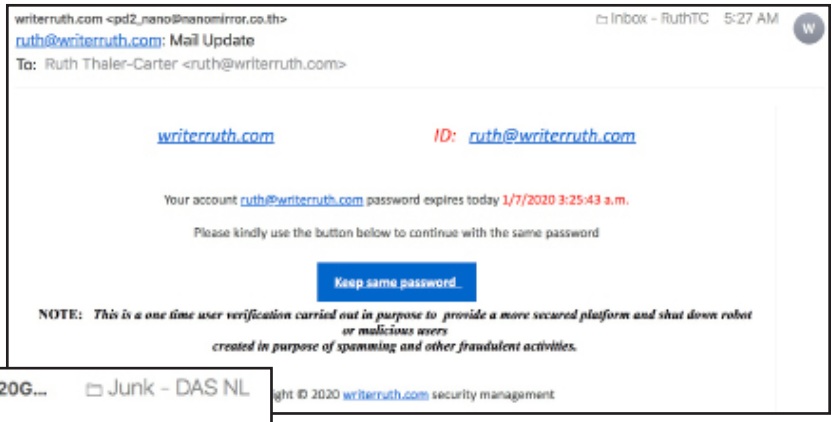
Being online is essential to our business lives, but it can be dangerous. Your website could be hacked and your accounts, information, computer and very reputation could be held at ransom.

Posts about ransomware

https://americaneditor.wordpress.com/?s=ransomware

Dangers

Spam
Scams (offers/actual checks or MOs for pay more than posted price of item for sale,
let "Microsoft" takes over computer to fix a virus, phony IRS collection calls)
Phishing
Hacking
Phony job offers (Google hangout interview)
Ransomware


writerruth.com <pd2_nano@nanomirror.co.th> Inbox - RuthTC 5:27 AM
ruth@writerruth.com: Mail Update
To: Ruth Thaler-Carter <ruth@writerruth.com>

writerruth.com ID: ruth@writerruth.com

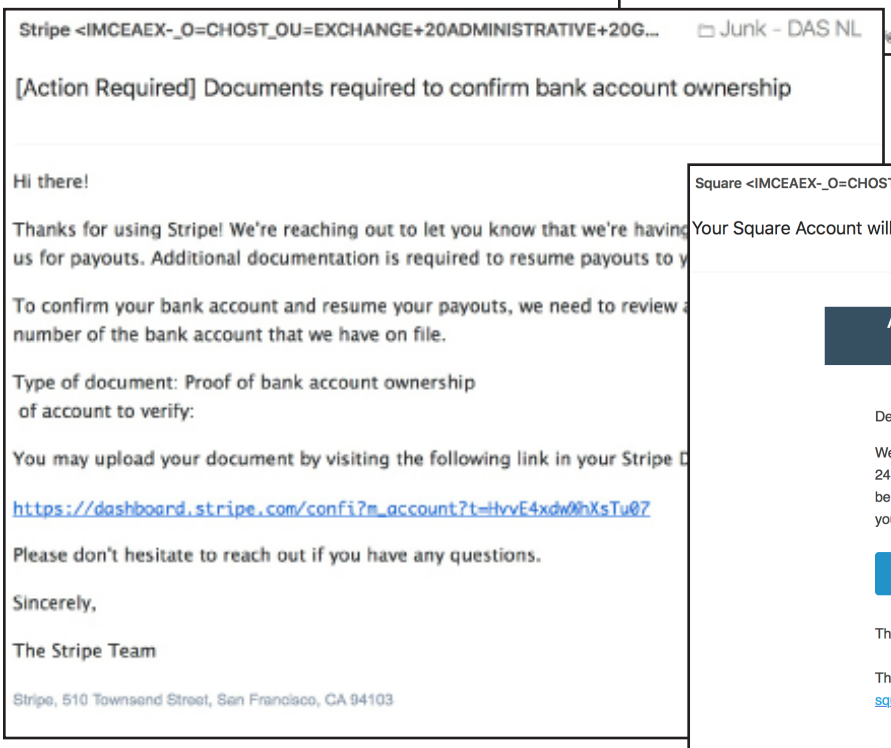
Your account ruth@writerruth.com password expires today 1/7/2020 3:25:43 a.m.

Please kindly use the button below to continue with the same password

Keep same password

NOTE: *This is a one time user verification carried out in purpose to provide a more secured platform and shut down robot or malicious users created in purpose of spamming and other fraudulent activities.*

ght © 2020 writerruth.com security management


Stripe <IMCEAEX-_O=CHOST_OU=EXCHANGE+20ADMINISTRATIVE+20G... Junk - DAS NL

[Action Required] Documents required to confirm bank account ownership

Hi there!

Thanks for using Stripe! We're reaching out to let you know that we're having
us for payouts. Additional documentation is required to resume payouts to y

To confirm your bank account and resume your payouts, we need to review a
number of the bank account that we have on file.

Type of document: Proof of bank account ownership
of account to verify:

You may upload your document by visiting the following link in your Stripe D

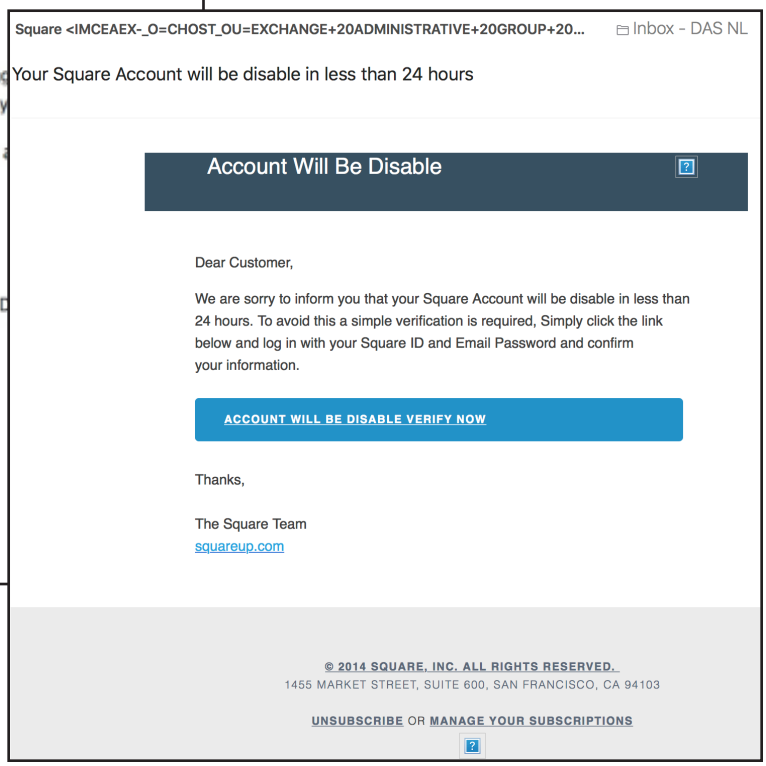
https://dashboard.stripe.com/confi?m_account?t=HvvE4xdW0hXsTu07

Please don't hesitate to reach out if you have any questions.

Sincerely,

The Stripe Team

Stripe, 510 Townsend Street, San Francisco, CA 94103


Square <IMCEAEX-_O=CHOST_OU=EXCHANGE+20ADMINISTRATIVE+20GROUP+20... Inbox - DAS NL

Your Square Account will be disable in less than 24 hours

Account Will Be Disable

Dear Customer,

We are sorry to inform you that your Square Account will be disable in less than 24 hours. To avoid this a simple verification is required, Simply click the link below and log in with your Square ID and Email Password and confirm your information.

ACCOUNT WILL BE DISABLE VERIFY NOW

Thanks,

The Square Team
squareup.com

© 2014 SQUARE, INC. ALL RIGHTS RESERVED.
1455 MARKET STREET, SUITE 600, SAN FRANCISCO, CA 94103

UNSUBSCRIBE OR MANAGE YOUR SUBSCRIPTIONS

Warning signs

- Clunky English
- Unknown senders
- Multiple recipients, especially if blind cc
- Links
- Requests to forward
- Job offers for things you don't do
- Job offers supposedly from major employers that include a Google Hangout interview
- "Friend requests" from strangers or people you're already connected to
- Offers of more than you usually charge or have listed
- Requests to purchase computers or other equipment with promises to reimburse
- Warnings or alerts from credit cards you don't own or banks you don't use
- Threats (especially in phone calls)

Save Yourself SaveYourself50@2810.com
I seen everything -

Hi, I know one of your passwords is:

Your computer was infected with my private malware, your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".

My malware gave me full access to all your accounts (see password above), full control over your computer and it also was possible to spy on you over your webcam.

I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!

After that I removed my malware to not leave any traces and this email(s) was sent from some hacked server.

I can publish the video of you and all your private data on the whole web, social networks, over email of all contacts.

But you can stop me and only I can help you out in this situation.

The only way to stop me, is to pay exactly 1000$ in bitcoin (BTC).

It's a very good offer, compared to all that horrible shit that will happen if I publish everything!

You can easily buy bitcoin here: www.paxful.com , www.coingate.com , www.coinbase.com , or check for bitcoin ATM near you, or Google for other exchanger.

You can send the bitcoin directly to my wallet, or create your own wallet first here: www.login.blockchain.com/en/#/signup/ , then receive and send to mine.

My bitcoin wallet is: 1Nq84HeDmd2JGyRtjqh32QRG4zoSrp8bdL

Copy and paste my wallet, it's (cAsE-sEnSEtiVE)

I give you 3 days time to pay.

As I got access to this email account, I will know if this email has already been read.

If you get this email multiple times, it's to make sure that you read it, my mailer script is configured like this and after payment you can ignore it.

After receiving the payment, I will remove everything and you can life your live in peace like before.

Next time update your browser before browsing the web!

Ways to protect yourself and your programs

1) Use robust passwords; update passwords every year and after any reported breach.
2) Use a password-storage program.
3) Don't share computers, programs or passwords.
4) Pay attention to reports of new breaches, scams and types of attacks.
5) Don't give in to threats!
6) Belong to professional organizations that will share/warn about scams.
7) Ask colleagues about fishy-seeming messages and offers.
8) Don't forward anything, including/especially on Facebook.
9) Don't answer the phone — legit callers will leave messages.
10) Don't deposit checks or money orders for more than what you charge or list.
11) **Never** give out ID info (SSN, etc.) on the phone or in e-mail unless you initiate the contact.
12) Don't pay more than you should — "invoices" for trademark and website domain/hosting renewals that look as if they're from legit agencies, but charge 10 times what you paid originally.

From the *Washington Post* (December 25, 2019) and IRS (https://www.irs.gov/newsroom/security-summit):

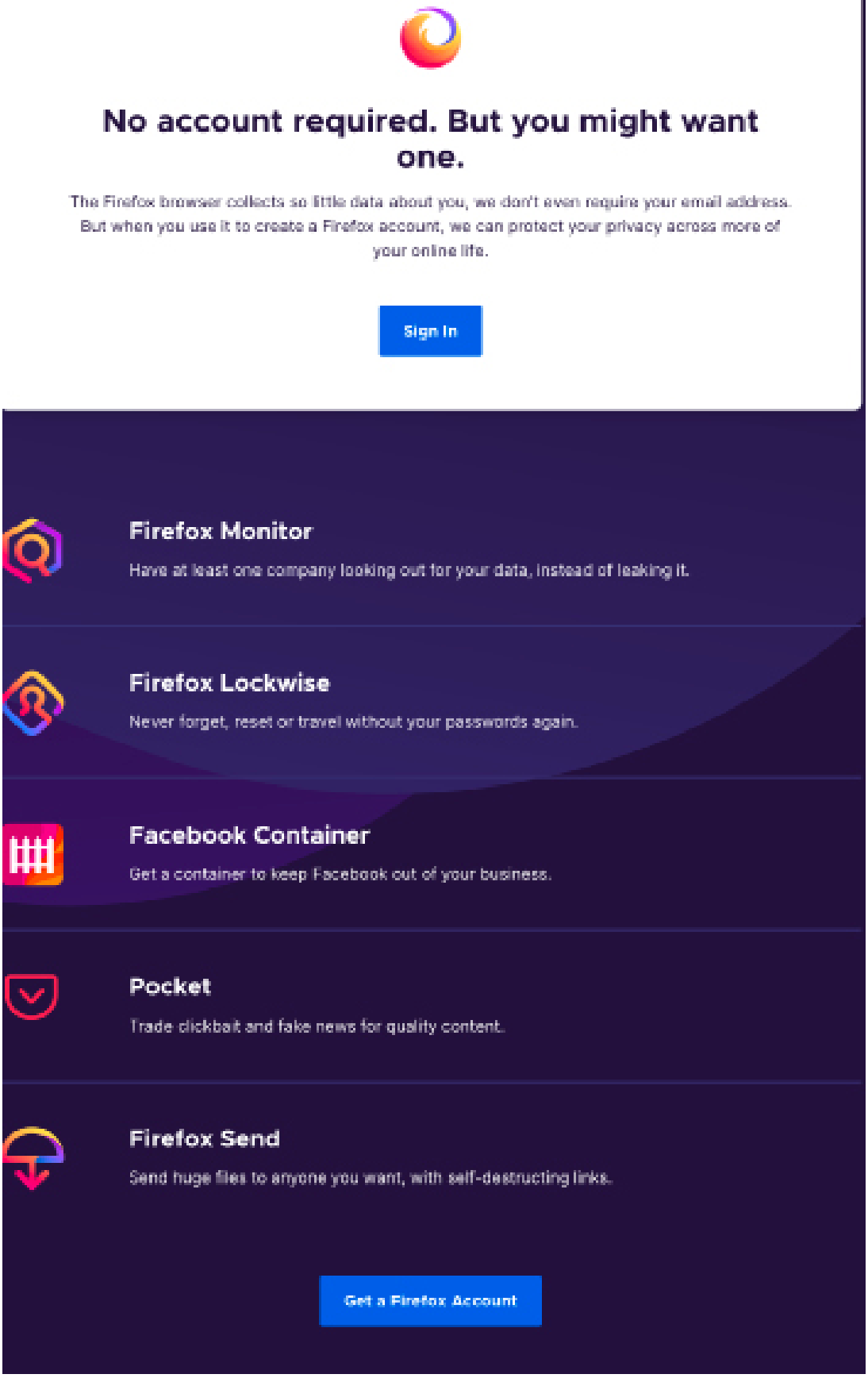
- Triple-check the URL at the top of the screen before making a purchase — make sure it has **https**, not just http (although scammers can and do use https, so double-check).
- Read reviews and check images for complaints about fraud or counterfeiting.
- Use a credit card or PayPal, Apple Pay or Samsung Pay, not a debit card.
- Use a temporary credit card whose number expires when a purchase is complete.
- Use common sense: If it looks too good to be true ($20 for a $2,00 luxury-brand item, or $2,000 for something you listed at $20), it probably is exactly that.
- Don't use unsecured WiFi at a coffee shop or hotel.
- Install anti-virus software that can stop malware.
- Have a firewall that can prevent intrusions.
- Use two-factor authentication.
- Back up all files.
- Don't open links or attachments on suspicious emails.

Tools to protect your computer

BitDefender Internet Security
Sandboxie
Firefox
LifeLock (Norton)
haveibeenpwned.com

Tools to protect your identity

Freeze requests to credit bureaus (Equifax, Experian, TransUnion)


No account required. But you might want one.
The Firefox browser collects so little data about you, we don't even require your email address. But when you use it to create a Firefox account, we can protect your privacy across more of your online life.
Sign In
Firefox Monitor
Have at least one company looking out for your data, instead of leaking it.
Firefox Lockwise
Never forget, reset or travel without your passwords again.
Facebook Container
Get a container to keep Facebook out of your business.
Pocket
Trade clickbait and fake news for quality content.
Firefox Send
Send huge files to anyone you want, with self-destructing links.
Get a Firefox Account