FRIENDS UNIVERSITY

Cyber Hygiene in a COVID World

How Social Distancing is Changing Security

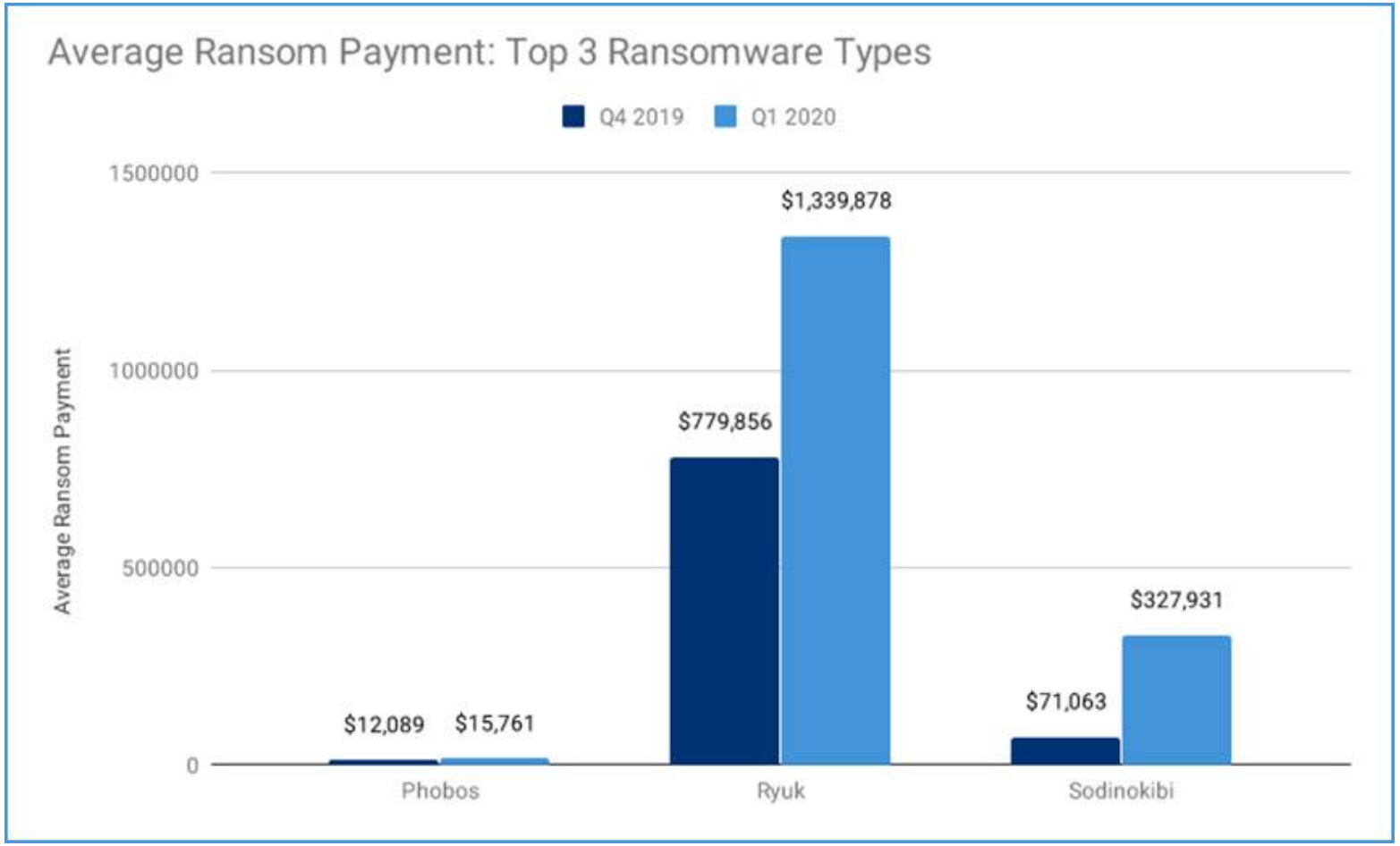
Overview

- SARS-CoV-2 / COVID-19 Pandemic Effect
- Social-Engineering & You
- Social Distancing & Cyber Security
- Better Security Practices
- Q&A

What is Changing: The Bad

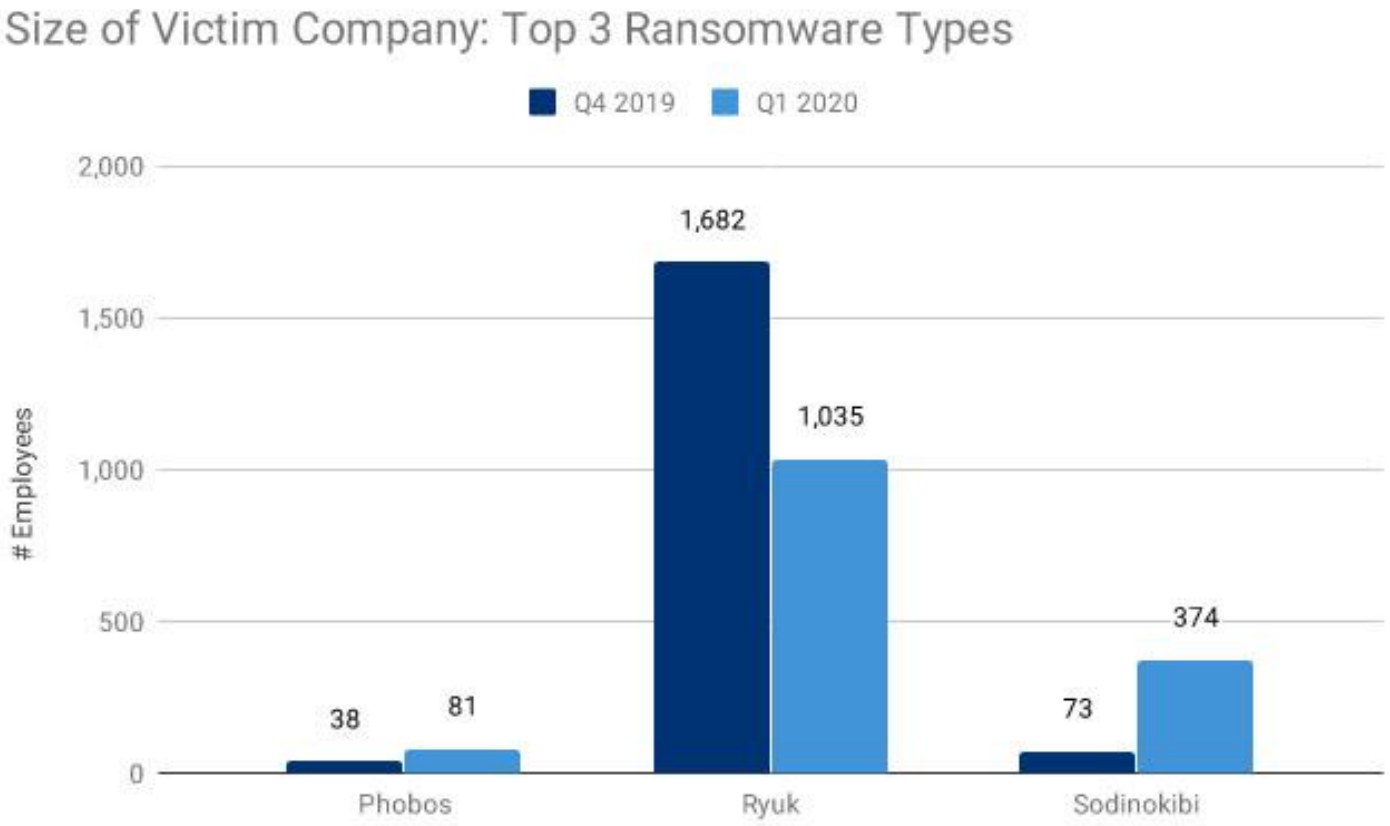
- More Phishing and Vishing attacks
- New physical security concerns
- Delayed attack detection / response
- More cyber-criminals … attempting to take advantage of circumstances

FRIENDS UNIVERSITY



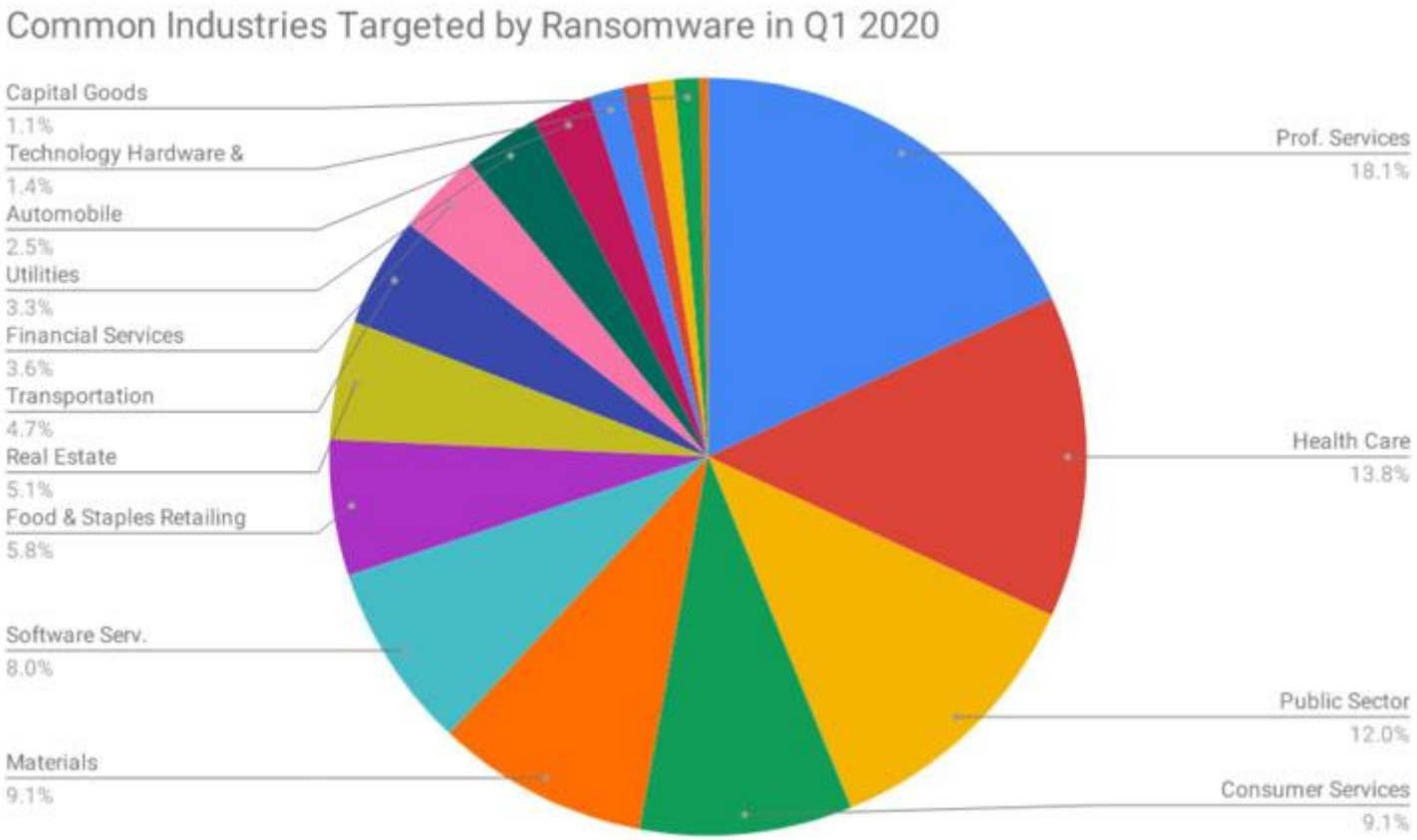
Source: Coveware

FRIENDS UNIVERSITY



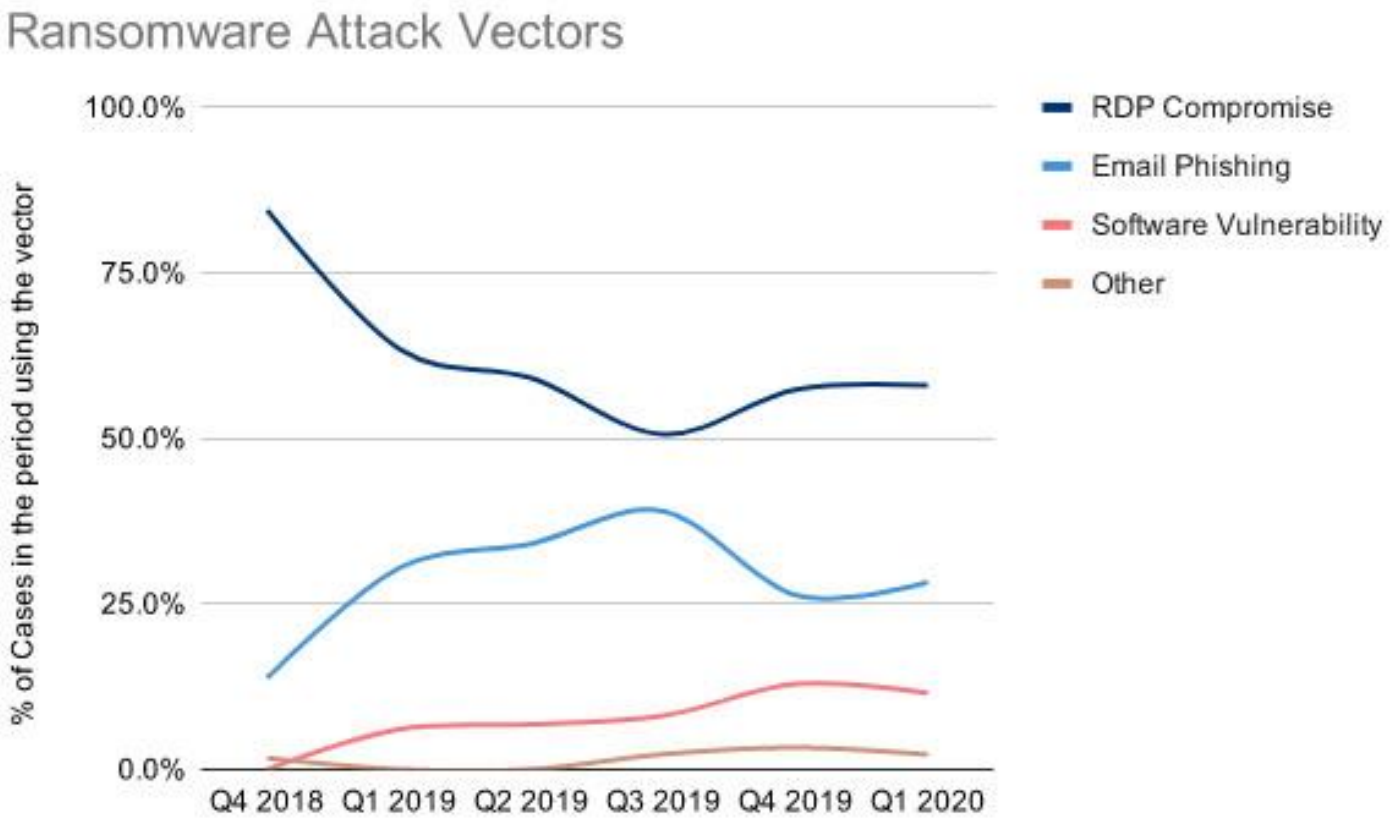
Source: Coveware

FRIENDS UNIVERSITY



Source: Coveware

FRIENDS UNIVERSITY



Source: Coveware

What is Changing: The Good

- More acceptance for remote / tele-work
- More / better employment of
- Rapid modification of security strategies for SMB
  - Zero-Trust environment adoption
  - VPN implementation / upgrade
  - Multi-Factor Authentication
  - Cloud-based capabilities

Social Engineering

What is it?

Social Engineering

- Social – human interactions (life)
- Engineering – (Latin & Greek origins) … to create … to be clever [to solve problems in a practical/applied way]

- Manipulation of people to enable perpetrators to action on objectives
- Take advantage of human nature to “get what you want”

Social Engineering

- Who does it:
  - Hackers
  - Pen-testers
  - Spies
  - Identity thieves
  - Employees
  - Con-men
  - Executive recruiters
  - Sales people
- Governments
- “Trusted” professionals

…

Social Engineering in Cyber Security

- Humans are the easiest target in an organization
- Most “relevant” data can be acquired in a combination of methods and mediums
- Breaches and compromise of defenses happen because of the people

Social Engineering Reconnaissance

- Information gathering in an unobtrusive manner
- Information is available and bountiful … bad guys use it
- Use every available source to understand a “target”
- Myriad of info gathering tools freely available to the “bad guy”

Reconnaissance

- Collection from the web:
  - What they do (about us)
  - Products & services
  - Physical locations
  - Job openings
  - Contact info
- Organization and leadership (the C-suite)
- Customer support
- Keyword & password/phrase clues
- Social media
- Public resources

Phishing, Vishing and Whaling (oh my!)

- Malicious activity utilizing email, text, telephone, or other messaging apparatus to target an individual or organization in an attempt acquire access to critical information or resources

Source: https://www.knowbe4.com/what-is-social-engineering/

FRIENDS UNIVERSITY

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

service@intl.paypal.com <service.epaiypal@outlook.com> 1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

FRIENDS UNIVERSITY

NETFLIX

We're sorry to say goodbye

Hello,

iTunes let us know that you asked to cancel your membership. We've cancelled your membership effective Tuesday, March 21st, 2017.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows & movies without interruption.

RESTART MEMBERSHIP

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

Questions? Call 1-866-579-7172

This account email has been sent to you as part of your Netflix

FRIENDS UNIVERSITY

Subject: Record Update.
From: "Dept. Of Labor" <records@dol.gov>
Date: 1/18/2016 1:57 PM
To: undisclosed-recipients:;

This is an urgent request to update your employment record at the U.S Department of Labor.

Update

Thank you

U.S Dept. of Labor
Frances Perkins Building,
200 Constitution Ave., NW,
Washington, DC 20210

FRIENDS UNIVERSITY

Urgent — Spear

Scott

To:

Reply-To:

Urgent

23 August 2016 15:43

SS

Hello Stuart,

Have you got a minute? I am currently tied up in a meeting. We need to facilitate a wire transfer to Indonesia for payment of an invoice Peter needs us to pay for today.

Let me know so I can pass across further information to you. Thanks.

Regards,
Scott

Sent from my iPhone

So What?

- People are the problem … and the solution!!
- Learn “what” to look for
- Don’t be afraid to question suspicious activity

What to Look For

- Urgency in the timing of the activity … something to scare you into action
- Unexpected/Unsolicited message
- Poor grammar, poor use of English, in appropriate familiarity
- Check the hyperlinks (website mismatch)
  - your-org.com … your-org.someothersite.com (.org, .biz, etc.)
- Sender address mismatch

FRIENDS UNIVERSITY

Social Engineering Red Flags

FROM

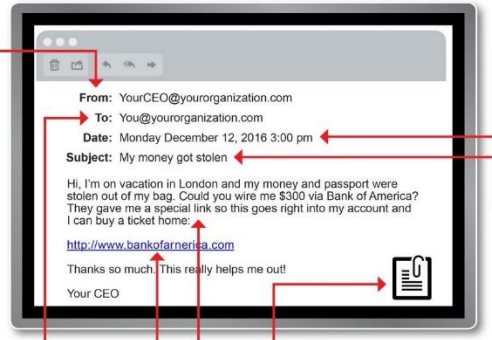
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4
Human error. Conquered.

Other Security Measures

- Implement / Use 2-Factor Authentication
  - Smartphone Apps:

  - 2FA Text Messaging
  - 2FA E-Mail

Other Security Measures

- Personal / business VPN implementation & use
- Zero-Trust in the remote ops business environment
  - Not just technology
  - Holistic Security Model
- Vulnerability Assessments
  - Not just scan results
  - Self Scan & 3rd Party Evaluation
- Get Help / Contract / Consultant

FRIENDS UNIVERSITY

Summary

- Social-Engineering & You
- Social Distancing & Cyber Security
- Better Security Practices
- Q&A

Questions

?