KB4-CON

Phish & Tips: Best Practices for Phishing Your Users

Katie Brennan, CISSP

Technical Content Director

KnowBe4

Agenda

- Introduction
- Phish inspiration
- Most interesting phishing techniques
- Best practices for phishing
- What’s new?
- Open discussion

Katie Brennan

- Technical Content Director
- Joined KnowBe4 in 2015
- Grew our template offering from 100 to over 3,000 in 40 languages/dialects
- Manages knowledge base
  - Wrote Best Practices guide

Phish Inspiration

How do we come up with our template ideas?

- My inbox
  - Anything can be weaponized
- Current events and scams
  - Politics, disasters, events, etc.
- Real phishing emails via the Phish Alert Button (PAB)
  - Over three million emails reviewed
  - Receiving 10,000-12,000 reported emails a day
  - Reported Phishes of the Week

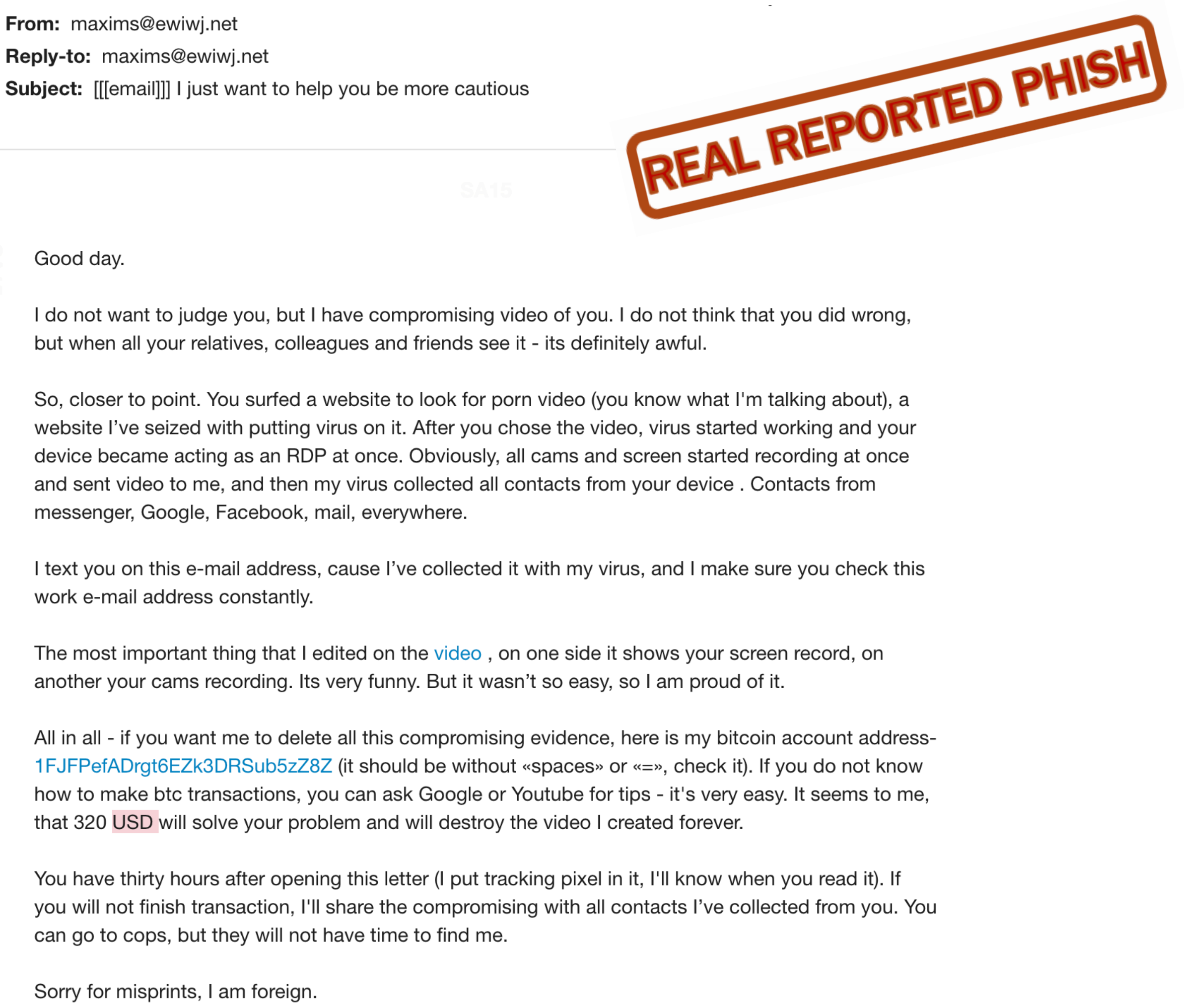
Most Interesting Phishing Techniques

What are the bad guys up to this year?

- Sextortion (with a twist)
- Online file sharing
- Fake attachments
- Fake text blocks
- Broken images
- Direct deposit scams
- Man-in-the-middle attacks
- HR-spoofed emails
- iTunes gift cards

Most Interesting Phishing Techniques: Sextortion

- Uses scare tactics to scam the user into sending them “hush” money



REAL REPORTED PHISH

From: maxims@ewiwj.net
Reply-to: maxims@ewiwj.net
Subject: [[[email]]] I just want to help you be more cautious

SA15

Good day.

I do not want to judge you, but I have compromising video of you. I do not think that you did wrong, but when all your relatives, colleagues and friends see it - its definitely awful.

So, closer to point. You surfed a website to look for porn video (you know what I'm talking about), a website I’ve seized with putting virus on it. After you chose the video, virus started working and your device became acting as an RDP at once. Obviously, all cams and screen started recording at once and sent video to me, and then my virus collected all contacts from your device . Contacts from messenger, Google, Facebook, mail, everywhere.

I text you on this e-mail address, cause I’ve collected it with my virus, and I make sure you check this work e-mail address constantly.

The most important thing that I edited on the video , on one side it shows your screen record, on another your cams recording. Its very funny. But it wasn’t so easy, so I am proud of it.

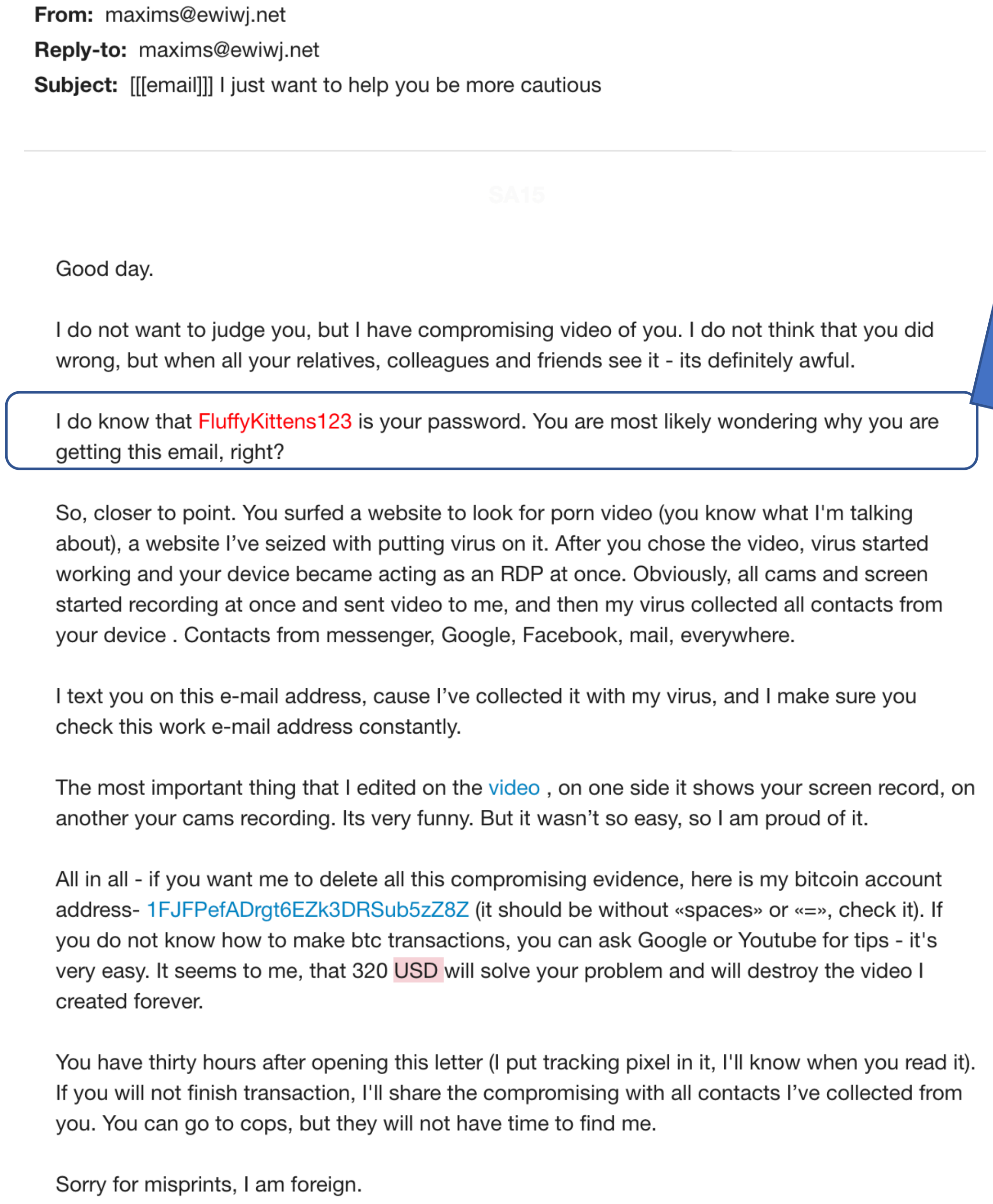
All in all - if you want me to delete all this compromising evidence, here is my bitcoin account address-1FJFPefADrgt6EZk3DRSub5zZ8Z (it should be without «spaces» or «=», check it). If you do not know how to make btc transactions, you can ask Google or Youtube for tips - it's very easy. It seems to me, that 320 USD will solve your problem and will destroy the video I created forever.

You have thirty hours after opening this letter (I put tracking pixel in it, I'll know when you read it). If you will not finish transaction, I'll share the compromising with all contacts I’ve collected from you. You can go to cops, but they will not have time to find me.

Sorry for misprints, I am foreign.

Most Interesting Phishing Techniques: Sextortion (with a twist!)

- Includes a real password that was involved in a data breach, to establish legitimacy and scare the user into reacting



From: maxims@ewiwj.net
Reply-to: maxims@ewiwj.net
Subject: [[[email]]] I just want to help you be more cautious

SA15

Good day.

I do not want to judge you, but I have compromising video of you. I do not think that you did wrong, but when all your relatives, colleagues and friends see it - its definitely awful.

I do know that FluffyKittens123 is your password. You are most likely wondering why you are getting this email, right?

So, closer to point. You surfed a website to look for porn video (you know what I'm talking about), a website I've seized with putting virus on it. After you chose the video, virus started working and your device became acting as an RDP at once. Obviously, all cams and screen started recording at once and sent video to me, and then my virus collected all contacts from your device . Contacts from messenger, Google, Facebook, mail, everywhere.

I text you on this e-mail address, cause I've collected it with my virus, and I make sure you check this work e-mail address constantly.

The most important thing that I edited on the video , on one side it shows your screen record, on another your cams recording. Its very funny. But it wasn't so easy, so I am proud of it.

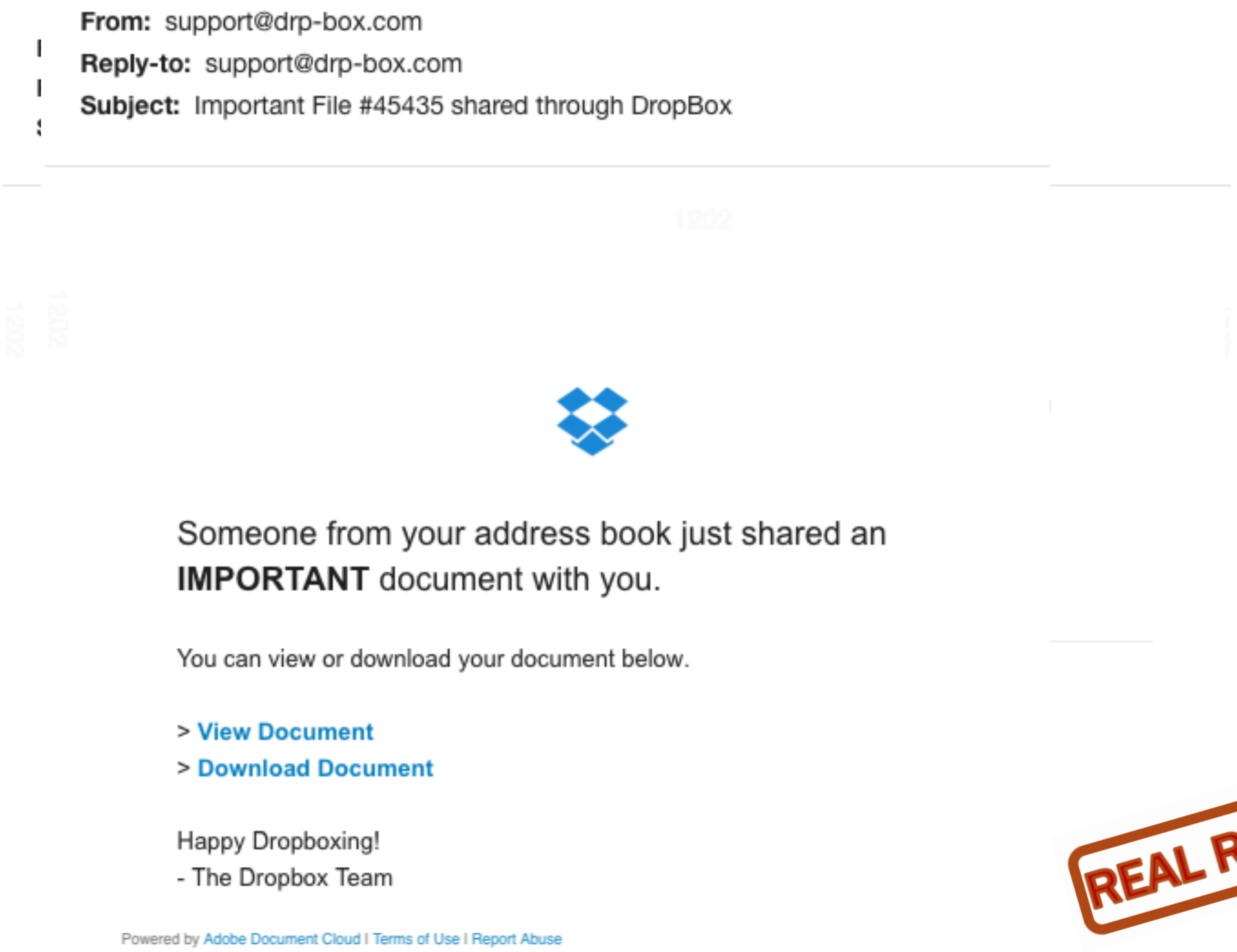
All in all - if you want me to delete all this compromising evidence, here is my bitcoin account address- 1FJFPefADrgt6EZk3DRSub5zZ8Z (it should be without «spaces» or «=», check it). If you do not know how to make btc transactions, you can ask Google or Youtube for tips - it's very easy. It seems to me, that 320 USD will solve your problem and will destroy the video I created forever.

You have thirty hours after opening this letter (I put tracking pixel in it, I'll know when you read it). If you will not finish transaction, I'll share the compromising with all contacts I've collected from you. You can go to cops, but they will not have time to find me.

Sorry for misprints, I am foreign.

Most Interesting Phishing Techniques: Online File Sharing

- Uses popular online file sharing platforms to share malicious files
- Notification comes directly from reputable the platform



From: support@drp-box.com

Reply-to: support@drp-box.com

Subject: Important File #45435 shared through DropBox

Someone from your address book just shared an **IMPORTANT** document with you.

You can view or download your document below.

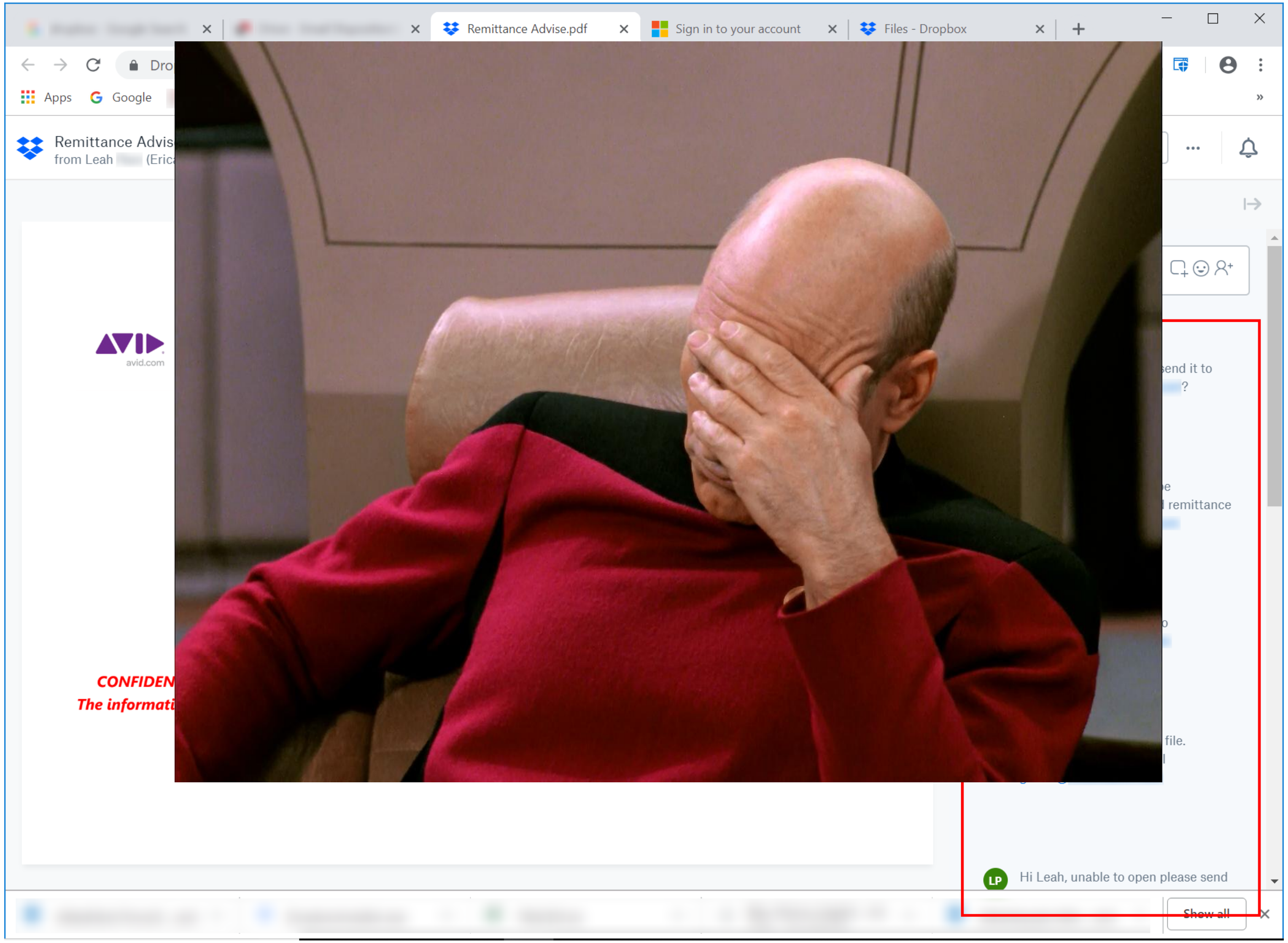
> View Document
> Download Document

Happy Dropboxing!
- The Dropbox Team

Powered by Adobe Document Cloud I Terms of Use I Report Abuse

REAL REPORTED PHISH

Most Interesting Phishing Techniques: Online File Sharing



Remittance Advise.pdf

Sign in to your account

Files - Dropbox

Dro

Apps

Google

Remittance Advis

from Leah [redacted] (Eric

avid.com

CONFIDEN

The informati

send it to

?

e

remittance

o

file.

LP

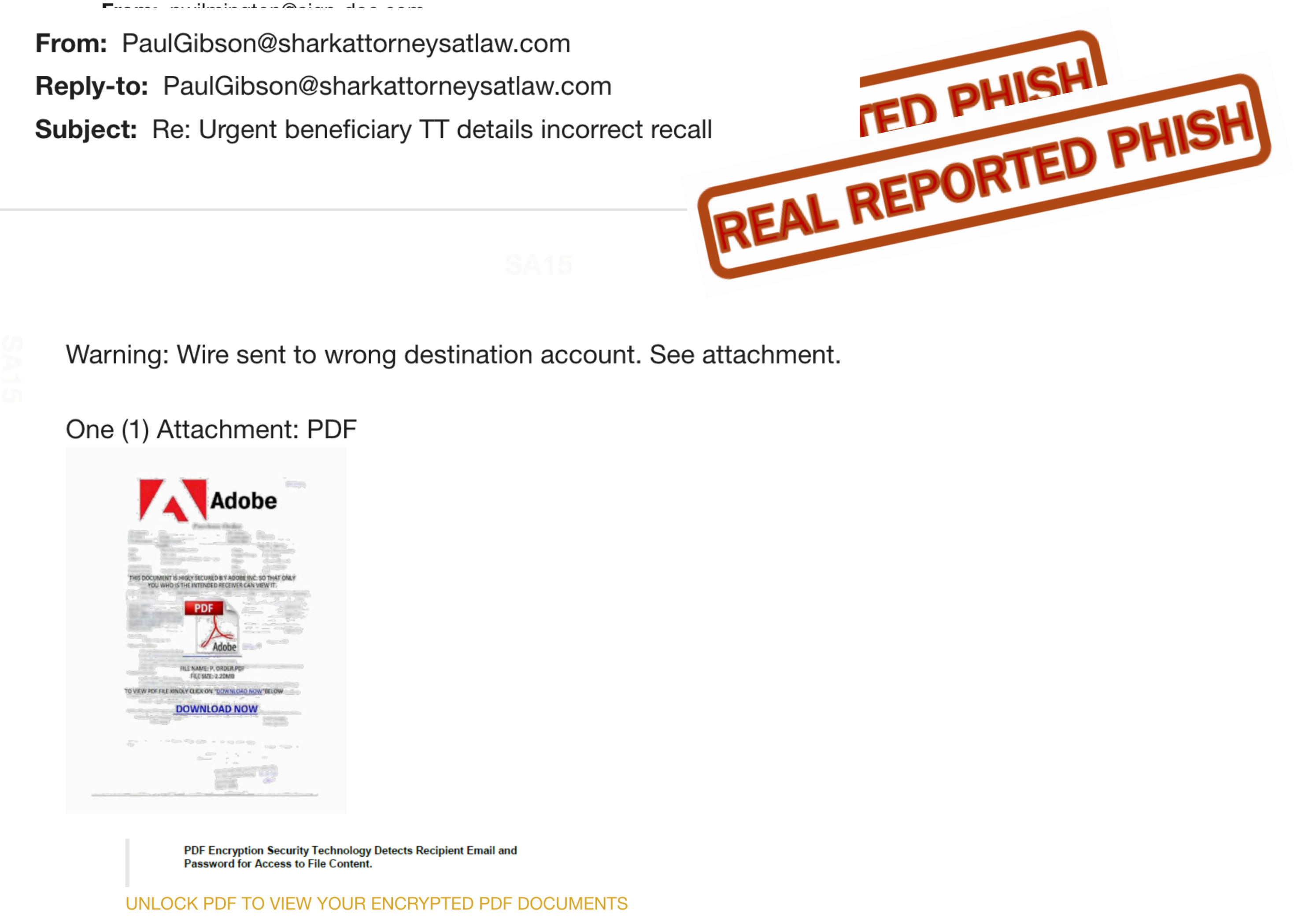
Hi Leah, unable to open please send

Show all

Most Interesting Phishing Techniques: Fake Attachments

- Uses images of attachments and text styling to mimic real attachments, but these are actually malicious links

- Many filters block attachments, so this is a workaround



From: PaulGibson@sharkattorneysatlaw.com

Reply-to: PaulGibson@sharkattorneysatlaw.com

Subject: Re: Urgent beneficiary TT details incorrect recall

Warning: Wire sent to wrong destination account. See attachment.

One (1) Attachment: PDF

Adobe

THIS DOCUMENT IS HIGLY SECURED B Y ADOBE INC. SO THAT ONLY YOU WHO IS THE INTENDED RECEIVER CAN VIEW IT.

PDF

Adobe

FILE NAME: P. ORDER.PDF
FILE SIZE: 2.20MB

TO VIEW PDF FILE KINDLY CLICK ON "DOWNLOAD NOW" BELOW

DOWNLOAD NOW

PDF Encryption Security Technology Detects Recipient Email and Password for Access to File Content.

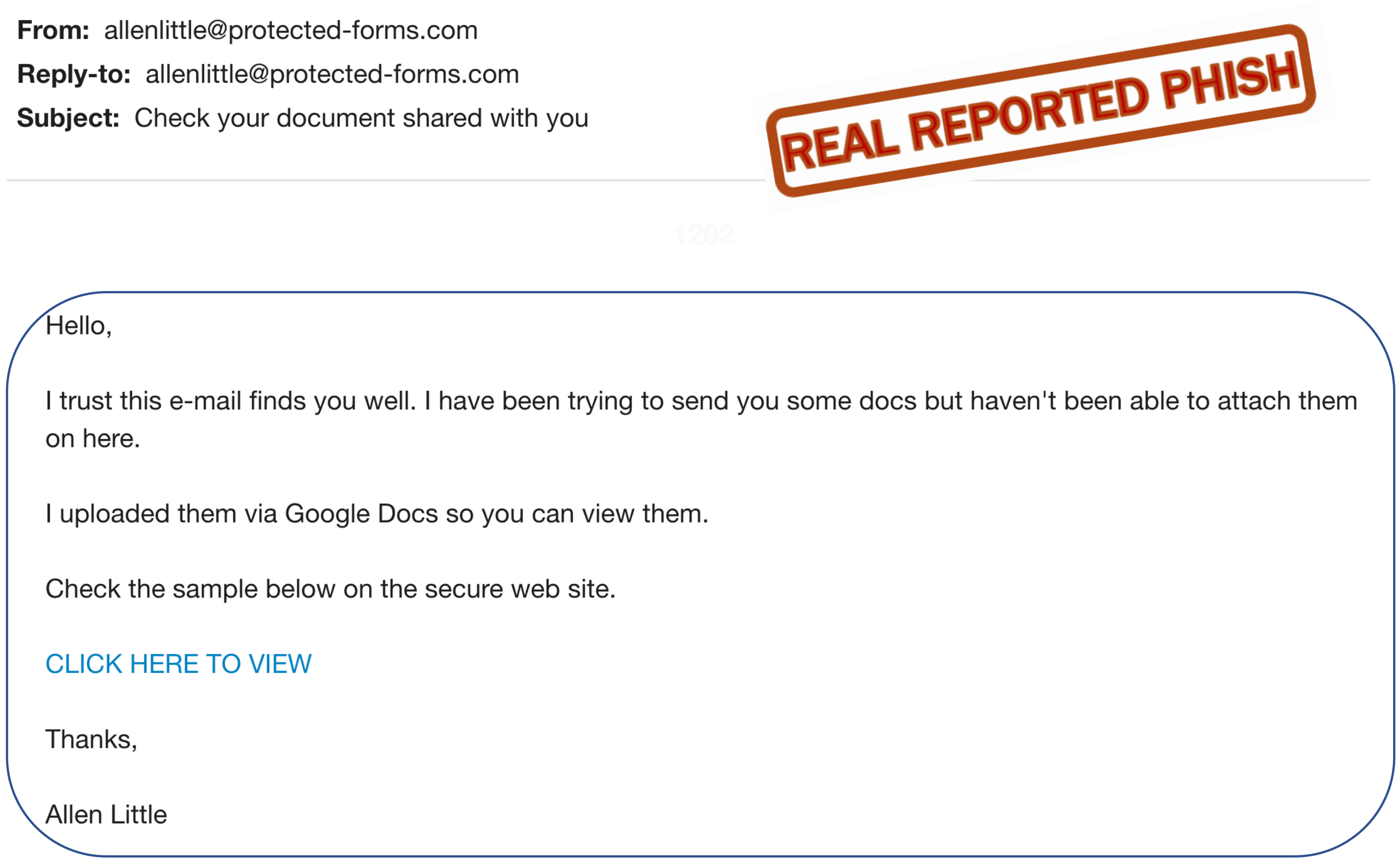
UNLOCK PDF TO VIEW YOUR ENCRYPTED PDF DOCUMENTS

TED PHISH

REAL REPORTED PHISH

Most Interesting Phishing Techniques: Fake Text Blocks

- Uses images of text to get phishy-sounding content past content filters
- The entire text block (image) is a link



From: allenlittle@protected-forms.com

Reply-to: allenlittle@protected-forms.com

Subject: Check your document shared with you

REAL REPORTED PHISH

Hello,

I trust this e-mail finds you well. I have been trying to send you some docs but haven't been able to attach them on here.

I uploaded them via Google Docs so you can view them.

Check the sample below on the secure web site.

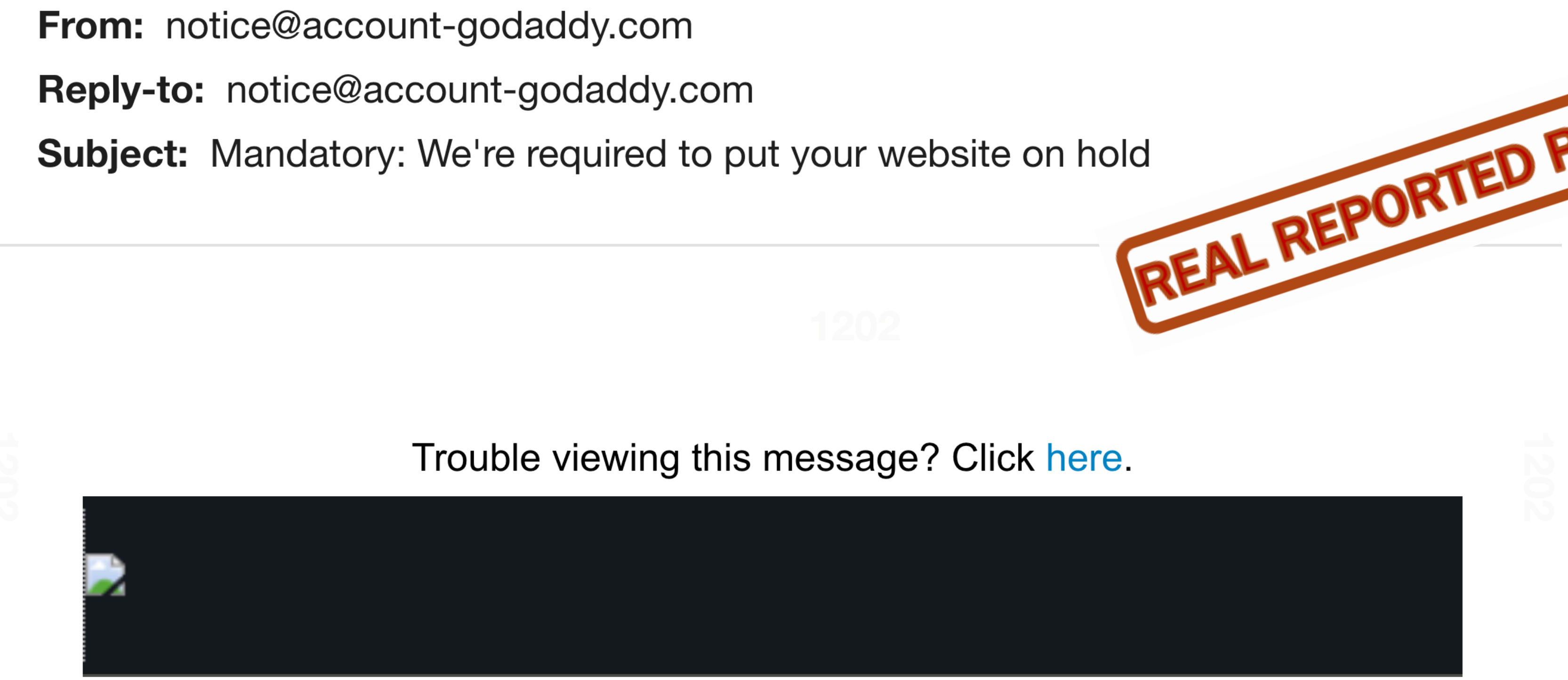
CLICK HERE TO VIEW

Thanks,

Allen Little

Most Interesting Phishing Techniques: Broken Images

- Uses a broken image on purpose combined with a helpful (malicious) link to get the user to click



From: notice@account-godaddy.com

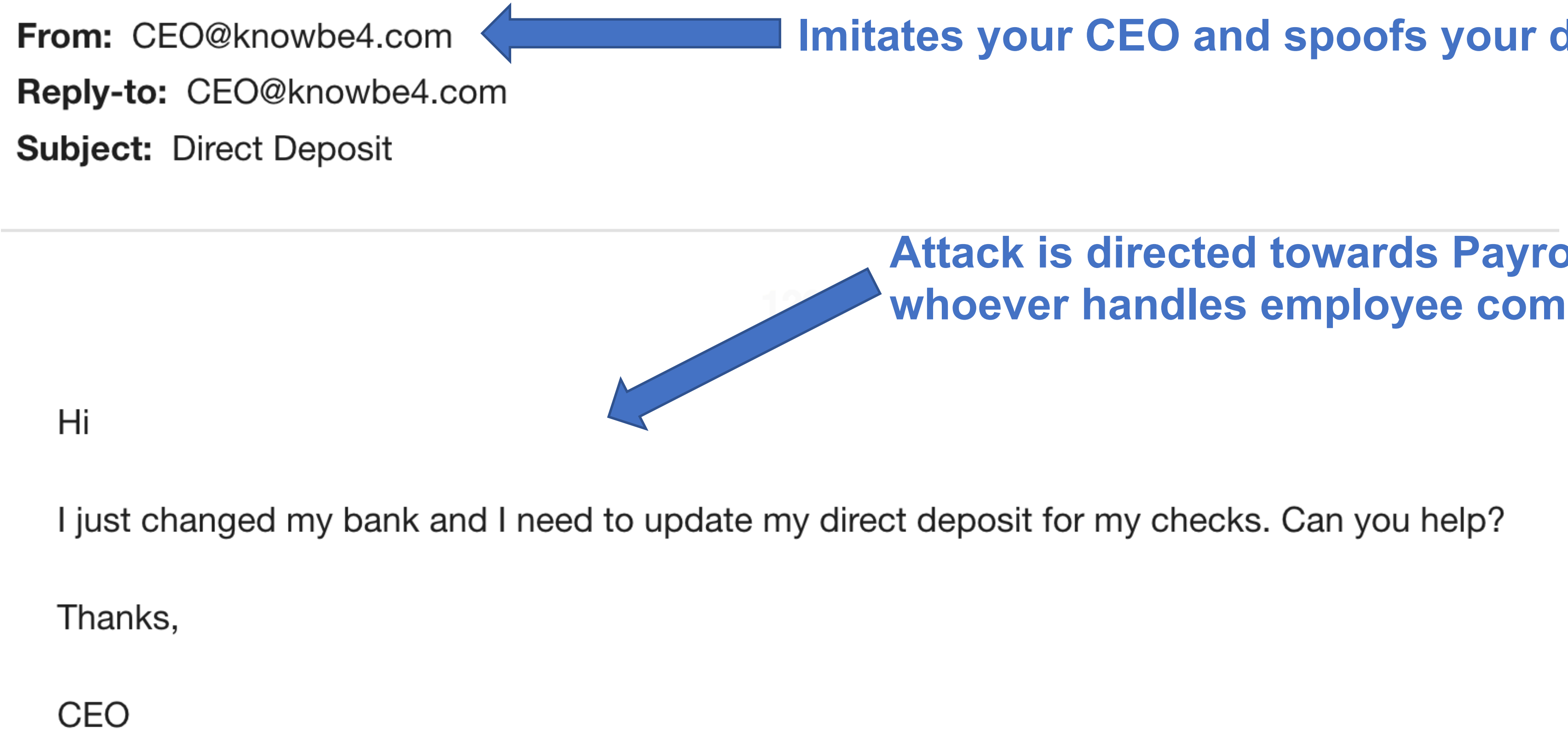
Reply-to: notice@account-godaddy.com

Subject: Mandatory: We're required to put your website on hold

Trouble viewing this message? Click here.

REAL REPORTED PHISH

Most Interesting Phishing Techniques: Direct Deposit



From: CEO@knowbe4.com

Reply-to: CEO@knowbe4.com

Subject: Direct Deposit

Hi

I just changed my bank and I need to update my direct deposit for my checks. Can you help?

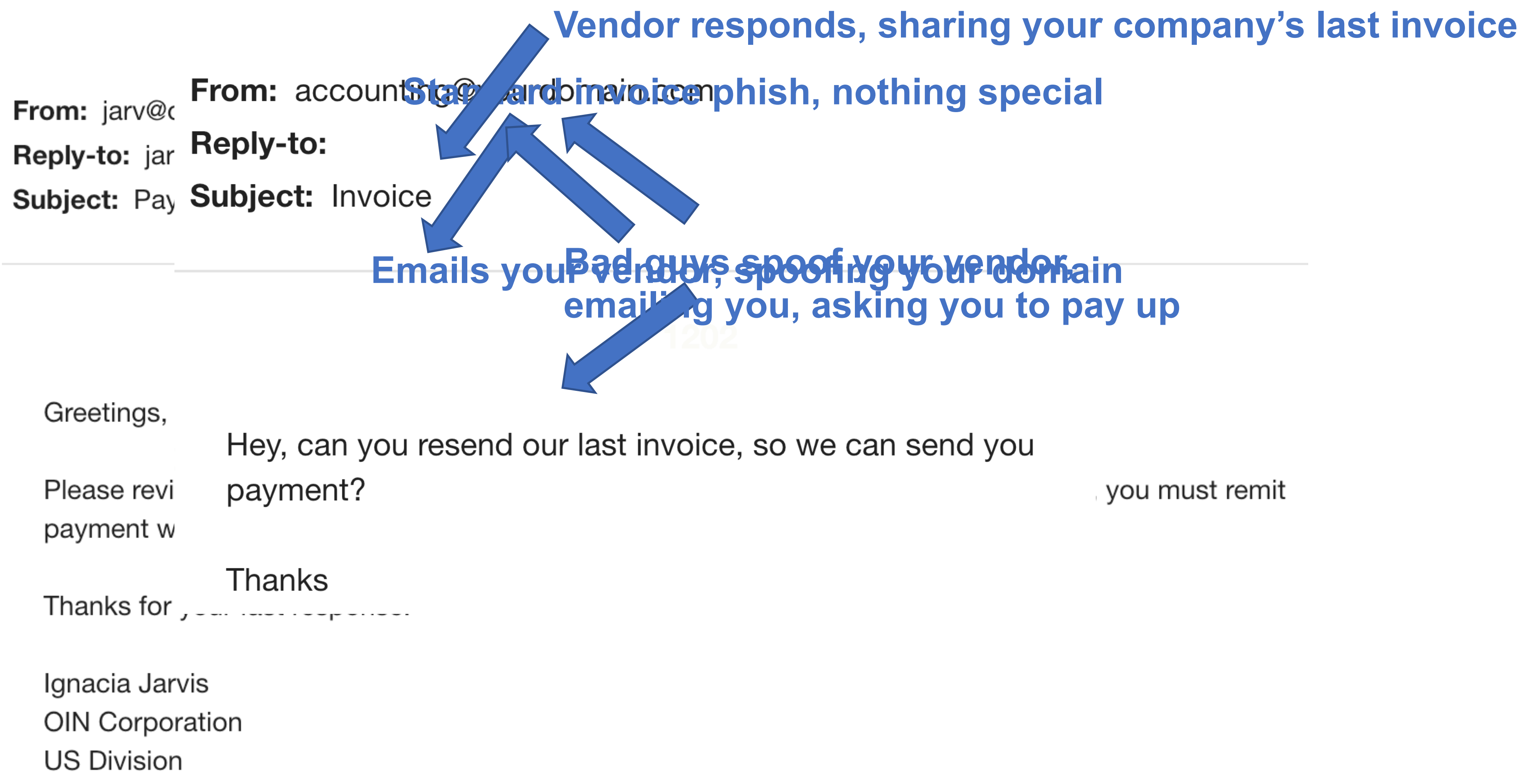
Thanks,

CEO

Imitates your CEO and spoofs your domain

Attack is directed towards Payroll, HR, or whoever handles employee compensation

Most Interesting Phishing Techniques: Man in the Middle



Vendor responds, sharing your company's last invoice

Standard invoice phish, nothing special

Emails your vendor, spoofing your domain

Bad guys spoof your vendor, emailing you, asking you to pay up

From: jarv@c
Reply-to: jar
Subject: Pay

Greetings,

Please revi you must remit
payment w

Thanks for

Ignacia Jarvis
OIN Corporation
US Division

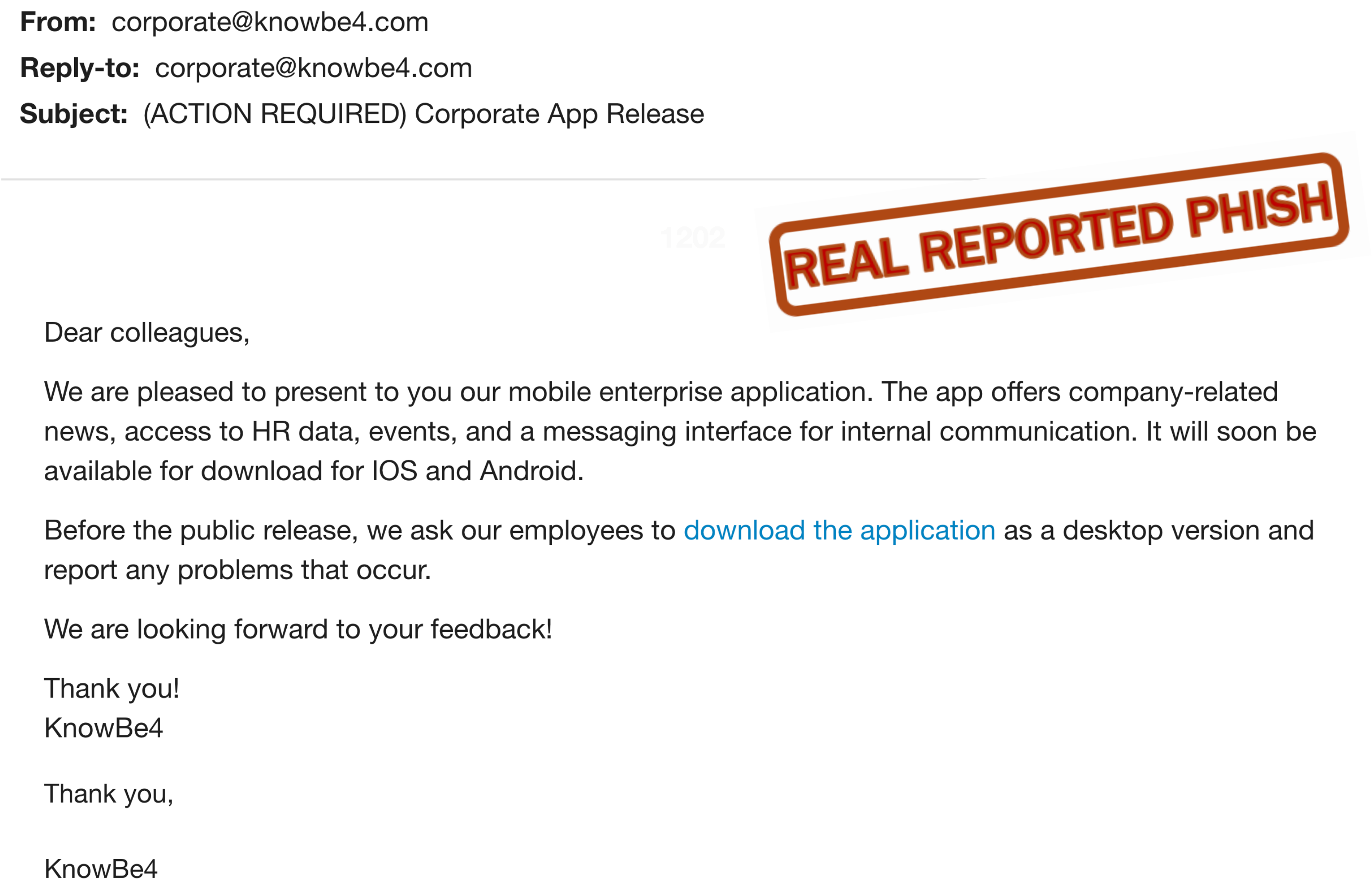
From: accounting@yourdomain.com
Reply-to:
Subject: Invoice

Hey, can you resend our last invoice, so we can send you payment?

Thanks

Most Interesting Phishing Techniques: Spoofed HR emails

- HR commands respect and authority, so HR emails are enticing for users to open
- Topics are usually of interest to users (PTO, performance reviews, payroll, benefits, etc.)



From: corporate@knowbe4.com

Reply-to: corporate@knowbe4.com

Subject: (ACTION REQUIRED) Corporate App Release

REAL REPORTED PHISH

Dear colleagues,

We are pleased to present to you our mobile enterprise application. The app offers company-related news, access to HR data, events, and a messaging interface for internal communication. It will soon be available for download for IOS and Android.

Before the public release, we ask our employees to download the application as a desktop version and report any problems that occur.

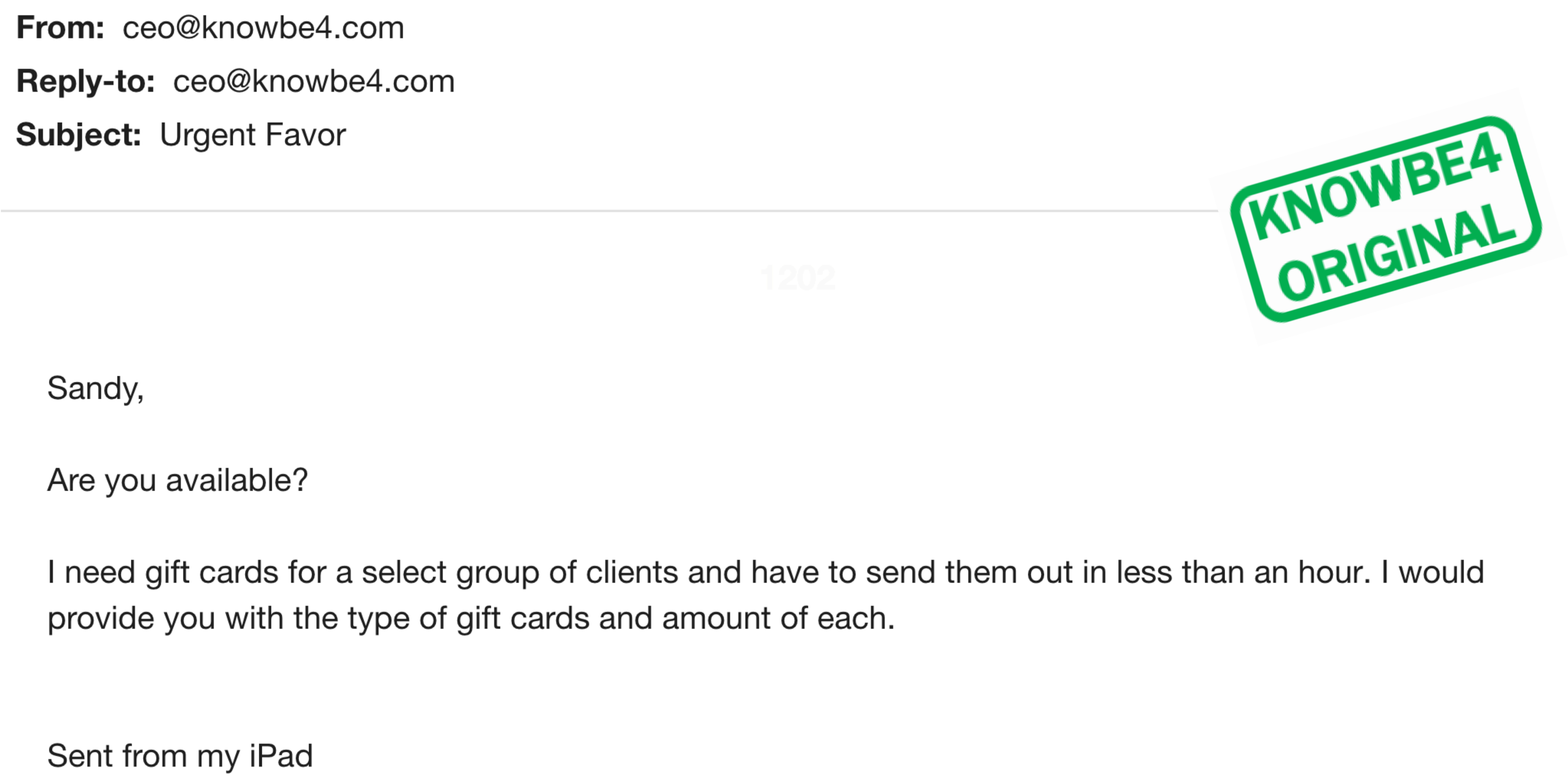
We are looking forward to your feedback!

Thank you!
KnowBe4

Thank you,

KnowBe4

Most Interesting Phishing Techniques: iTunes Gift Cards



From: ceo@knowbe4.com

Reply-to: ceo@knowbe4.com

Subject: Urgent Favor

KNOWBE4 ORIGINAL

1202

Sandy,

Are you available?

I need gift cards for a select group of clients and have to send them out in less than an hour. I would provide you with the type of gift cards and amount of each.

Sent from my iPad

Most Interesting Phishing Techniques: iTunes Gift Cards

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

Hi Emily, Let me know when you are available. There is something I need you to do.

I am going into a meeting now with limited phone calls, so just reply to my email.

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

Did you intend to send this to me?

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

Yes Emily, can you get this done ASAP? I need some couple of gift cards.

There are some listed clients we are presenting the gift cards. How quickly can you arrange these gift cards because i need to send them out in less than an hour. I would provide you with the type of gift cards and amount of each..

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

Can do now. I'll put on my credit card. Send me the following:

Type
Number
Amount

Most Interesting Phishing Techniques: iTunes Gift Cards

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

The type of card I need is Apple iTunes gift cards. $100 denomination, I need $100 X 20 cards. You might not be able to get all in one store, you can get them from different stores. When you get the cards, Scratch out the back to reveal the card codes, and email me the codes. How soon can you get that done? Its Urgent.

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

On my way to store now. What time do you need them by?

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

As soon as you can. I will await codes

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>

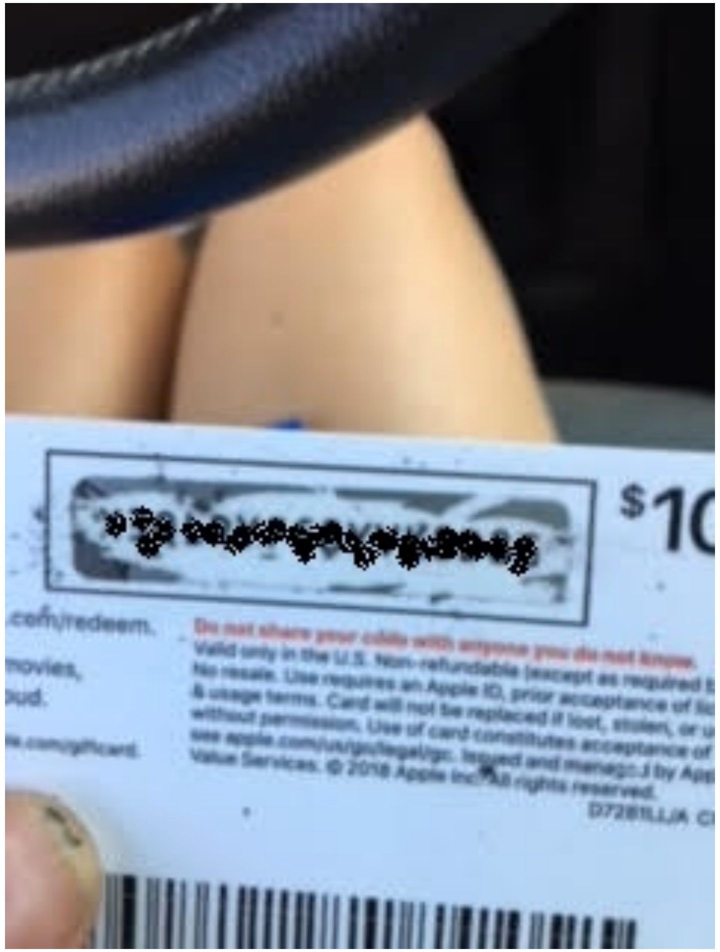
Just texted you the first 11 codes. Heading to another store now. 5 and 6 limit per store.

Most Interesting Phishing Techniques: iTunes Gift Cards

From: John Carpenter <officeexec.mails@inbox.lv>
To: Emily Walker <ewalker@distracted.com>

Email them to me

From: Emily Walker <ewalker@distracted.com>
To: John Carpenter <officeexec.mails@inbox.lv>


[redacted]
$10
.com/redeem.
movies,
oud.
e.com/giftcard.
Do not share your code with anyone you do not know.
Valid only in the U.S. Non-refundable (except as required b
No resale. Use requires an Apple ID, prior acceptance of lic
& usage terms. Card will not be replaced if lost, stolen, or u
without permission. Use of card constitutes acceptance of
see apple.com/us/go/legal/gc. Issued and managed by App
Value Services. © 2018 Apple Inc. All rights reserved.
D7281LL/A C

Best Practices

Best Practices for Phishing Your Users

1. Prepare to “go phishing”
2. Decide what to do **after** you phish (***before*** you phish!)
3. Conduct your **baseline** phishing test
4. Start **ongoing** phishing
5. Check in on your **progress** and adapt your program

Best Practices for Phishing Your Users

1. Prepare to “go phishing”

- Automated Security Awareness Program (ASAP)
- **Engage your stakeholders** to cultivate your organization’s security awareness culture
- Plan how you’ll set up **users and user groups**
  - Reporting, Targeting
  - Smart Groups
- Use your **resources** along the way
  - KnowBe4 Support or your Customer Success Manager (CSM)

Best Practices for Phishing Your Users

2. Decide what to do after you phish (before you phish!)

- Will you **inform** your users or **share** the results of your baseline test?
  - Reinforce the importance of your plan

- Introduce an **incident response plan** for phishing emails
  - Phish Alert Button (PAB)

- Consider how to train or handle your **most vulnerable** users
  - Remedial Training with short modules
  - Social Engineering Indicators (SEI)

Best Practices for Phishing Your Users

3. Conduct your baseline phishing test

- Use a **generic** template
  - Categories: Baseline Templates, Human Resources, IT
- Send the templates **all at once**
  - Reduces the “prairie dog” effect
- Warn **only** those who need to know
  - IT, who may receive lots of forwarded “phishing” emails
  - If you’re spoofing HR, IT, or anyone else—let them in on it!

Best Practices for Phishing Your Users

4. Start an ongoing phishing program

- Conduct **weekly**, **biweekly**, or **monthly** phishing
  - Keeps security at top of mind

- Ramp up your **phishing difficulty** over time
  - Difficulty Rating
  - Set up tiered phishing using Smart Groups (Platinum/Diamond) – vulnerable users get phished more often automatically!

- Vary your phishing template **attack vectors** – anything can be weaponized
  - Maximize variability – keep your users guessing

- Stick to what the hackers use…**most** of the time
  - Hackers still rely on old techniques and distracted or untrained users

Best Practices for Phishing Your Users

5. Check in on your progress and adapt

- Platform can be **set it and forget it**, but that doesn’t mean you should forget it
  - Review reports and find out:
    - Where are your users the most vulnerable?
    - What types of templates are they clicking on?

- Set up **targeted** phishing and training for vulnerable users or departments
  - Phish-prone users
  - Accounting, HR, Help Desk, Executives

- Consider adding penalties for failing phishing tests in your company policies

What techniques do hackers use *most* of the time?

According to our research, around **90%** of the emails that are reported to us use social engineering schemes that have been around for many years.

Fake invoices, POs, and RFQs "Your invoice is past due. Click here to pay it now."

Fake package or parcel delivery notifications

Fake file delivery, sharing, or signing notifications

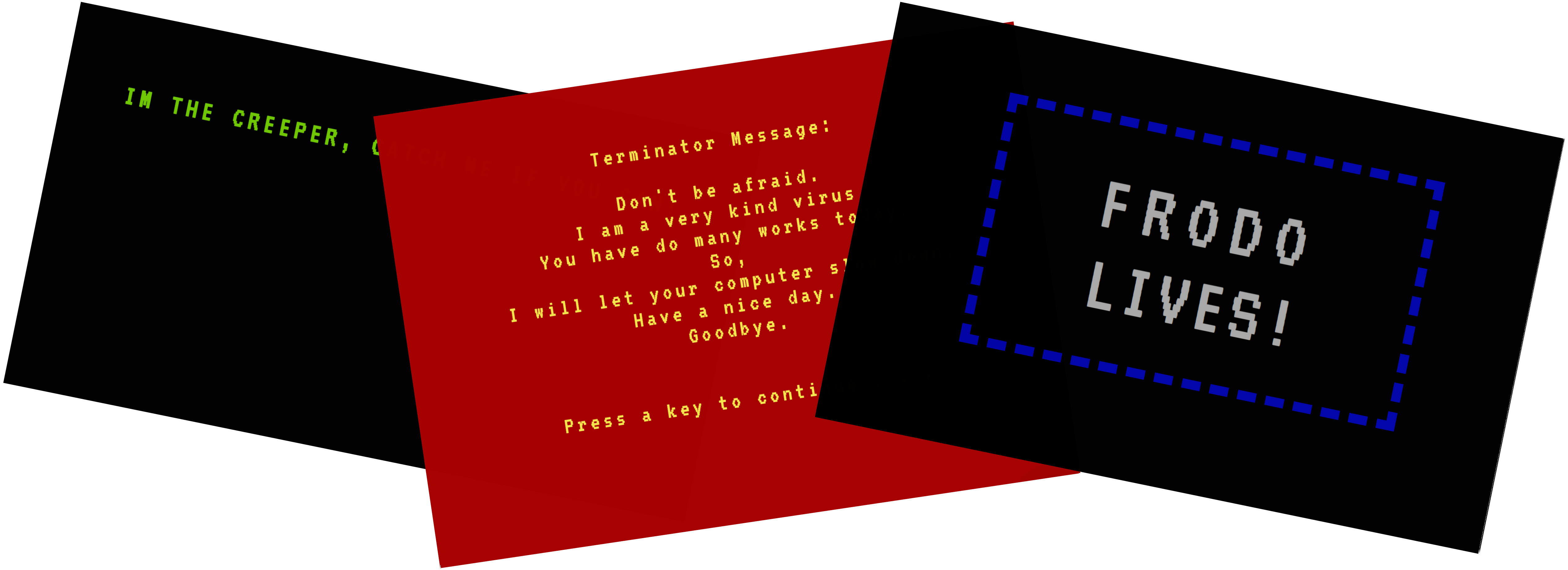
Email upgrade/update notifications "Upgrade your email or ALL of your email will be deleted. UPGRADE NOW."

Email password expiration notifications "Your password is expired. Create your new password so you can log in."

Bogus online account "verifications" or "updates"

Email deactivation warnings "Your email will be deactivated if you don't click here to cancel deactivation."

What’s new? Ransomware Landing Pages



IM THE CREEPER, C

Terminator Message:

Don't be afraid.
I am a very kind virus
You have do many works to
So,
I will let your computer s
Have a nice day.
Goodbye.

Press a key to conti

FRODO LIVES!

Thank You!

Katie Brennan, Technical Content Director

KnowBe4

Tips For Your Users

- Don’t reply or forward
- Know the signs of a safe email just as much as the signs of a dangerous email
- Understand the parts of a web address
  - What to look for when hovering
- Look out for these signs of a phishing attack:
  - Brand mismatch
  - Typos
  - URL shorteners