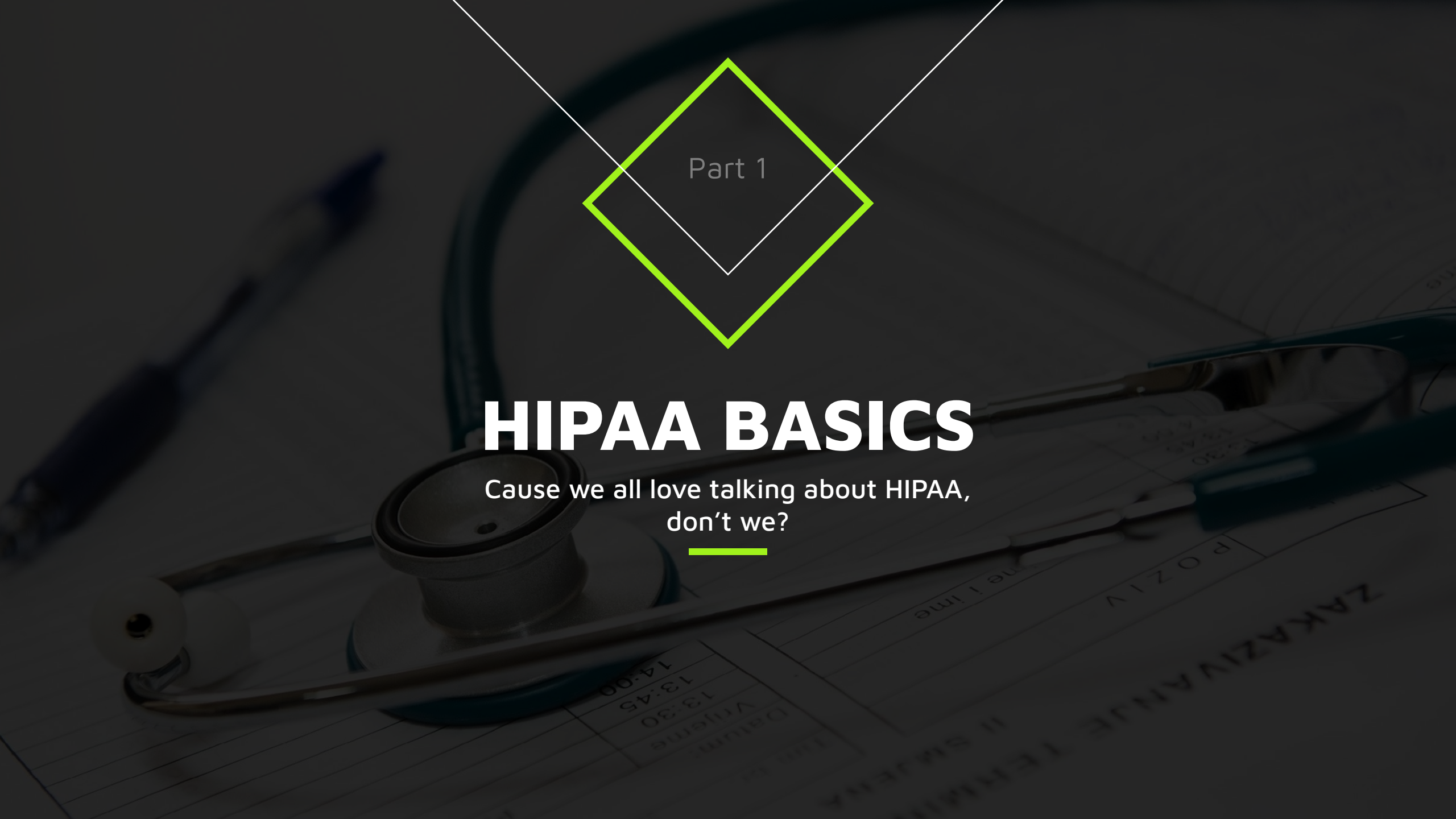


Part 1

HIPAA BASICS

Cause we all love talking about HIPAA,
don’t we?

BACK TO BASICS

Lets review!

Protected Health Information

Covered Entity

Business Associate

BACK TO BASICS

Lets review!

Protected Health Information

Covered Entity

Business Associate

PROTECTED HEALTH INFORMATION (PHI)

Any information that can be used to identify a patient, living or dead.

BACK TO BASICS

Lets review!

Protected Health Information

Covered Entity

Business Associate

COVERED ENTITY

Any individual, organization, or corporation that directly handles PHI.

BACK TO BASICS

Lets review!

Protected Health Information

Covered Entity

Business Associate

BUSINESS ASSOCIATE

Any individual, organization, or corporation that performs functions or provides services for covered entities

BACK TO BASICS

Privacy Rule

When can you disclose PHI?

Required

When the patient/patient's representative or HHS asks for it

Permitted

When it's for the purposes of Treatment, Payment, or Healthcare Operations

Authorized

When a valid authorization letter is presented

Privacy Rule

When can you disclose PHI?

MINIMUM NECESSARY RULE

Regardless if it's Required, Permitted, or Authorized, only disclose the necessary information to achieve the goal

BACK TO BASICS

Security Rule

Protecting electronic PHI (e-PHI)

Administrative safeguards

HIPAA trainings, HIPAA-related company policies, HIPAA Security and Legal officers

Physical safeguards

Biometrics, magnetic doors, locked server rooms, role-based working space

Technical safeguards

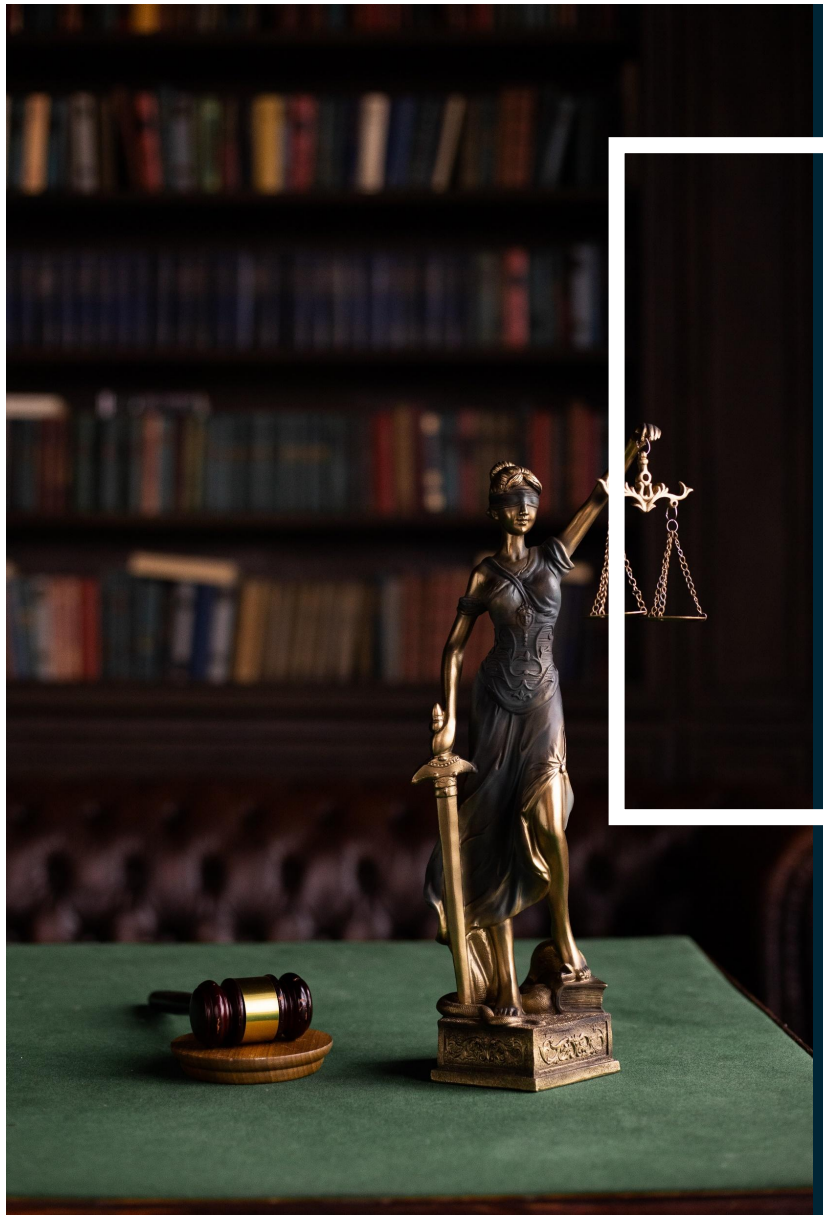
Company VPN, Firewall, Encryption programs, Internet access control and auditing

Part 2

PATIENT RIGHTS

What? I thought we were talking about HIPAA?

PATIENT RIGHTS



Patients have rights.

Legal rights.

That is why we, as a company, are accountable in how we handle a patient's PHI.

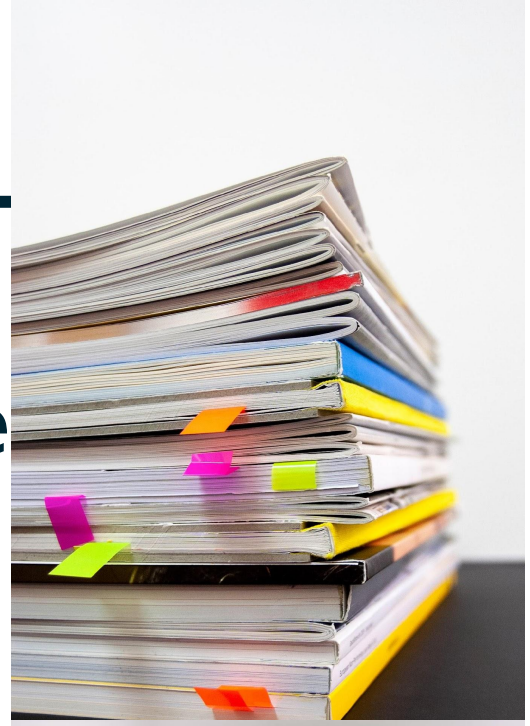
The right to get their entire medical record.

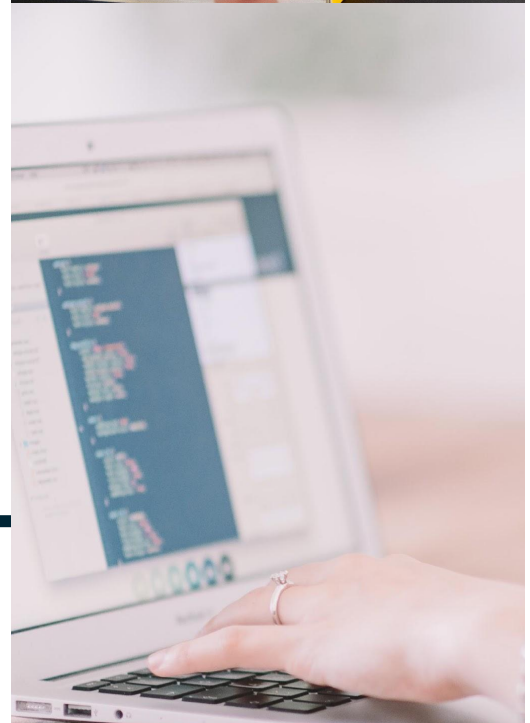
This includes all medical notes, billing notes, and all other records.

PATIENT RIGHTS

The right to have their records in their preferred format.

This includes sending it through their preferred method as well.





IF SENT VIA EMAIL

Email must either be encrypted or a Notice Warning must be provided to explicitly warn the patient the risk of emails being intercepted.

IF ASKED THROUGH A CALL

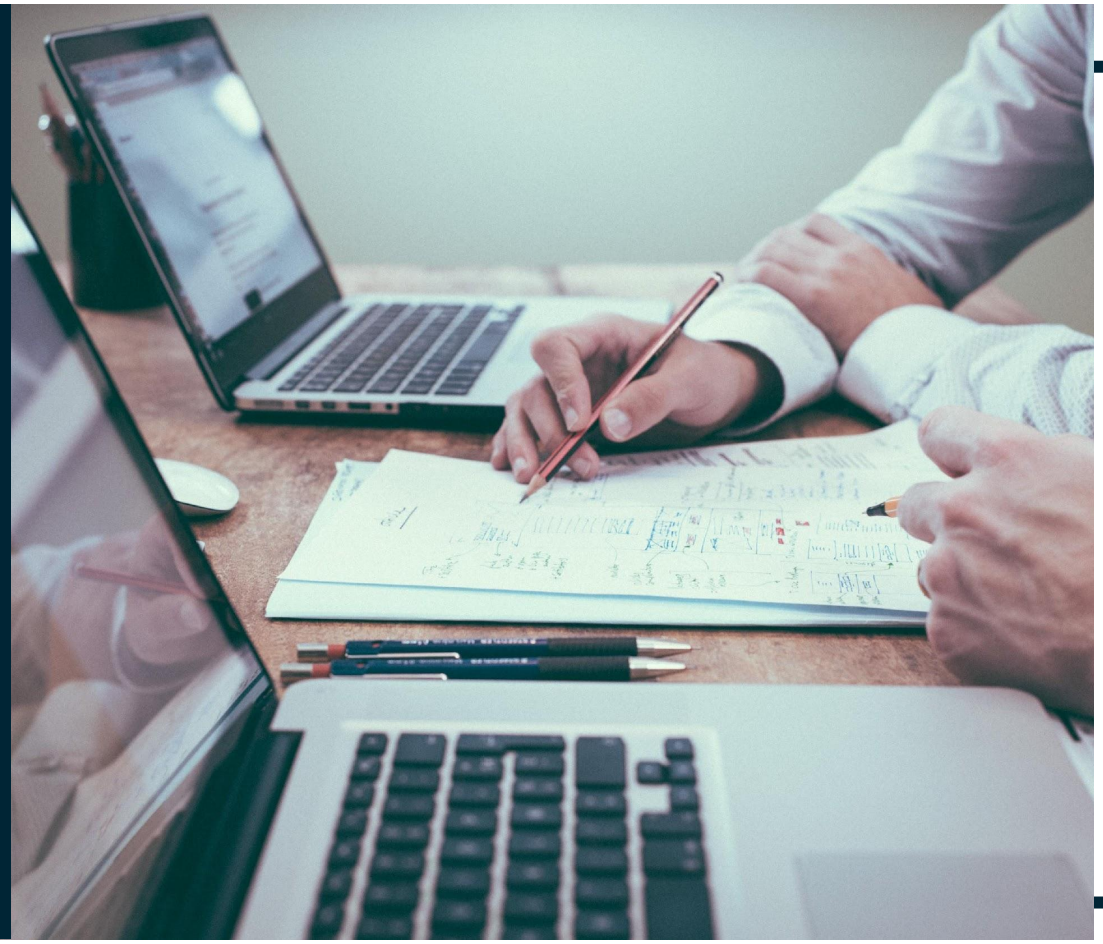
An identity verification procedure must be done before verbalizing the PHI.

The right to inspect and review their medical records.

This includes viewing the records the same way they are shown in the office.

The right to accounting of disclosures.

This includes information on where we've sent their records for the past six years.



Part 3

CYBERSECURITY

Why? Because you’re still not locking your computer!

CYBERSECURITY

45%

Increase in cyberattacks since COVID began

1,126
Attempted cyber attacks in the last quarter of 2021

542
Successful attempts in the same period

213
Led to identity-related crimes and fraud

SELF-INFLICTED BREACHES

Records mistakenly sent to a wrong patient

Employee snooping and gossiping

Wrong attachments

Improper disposal of records

BREACH NOTIFICATION

1. Report potential breaches to HR. Do not wait for them to actually happen

2. HR will conduct an investigation, possibly together with the Security and Compliance team.

3. Appropriate hearings and sanctions will be doled out to the responsible parties.

FORMULA TO AVOID CIVIL PENALTIES

Establishing company policies and safeguards

+

Executing business associate agreements

+

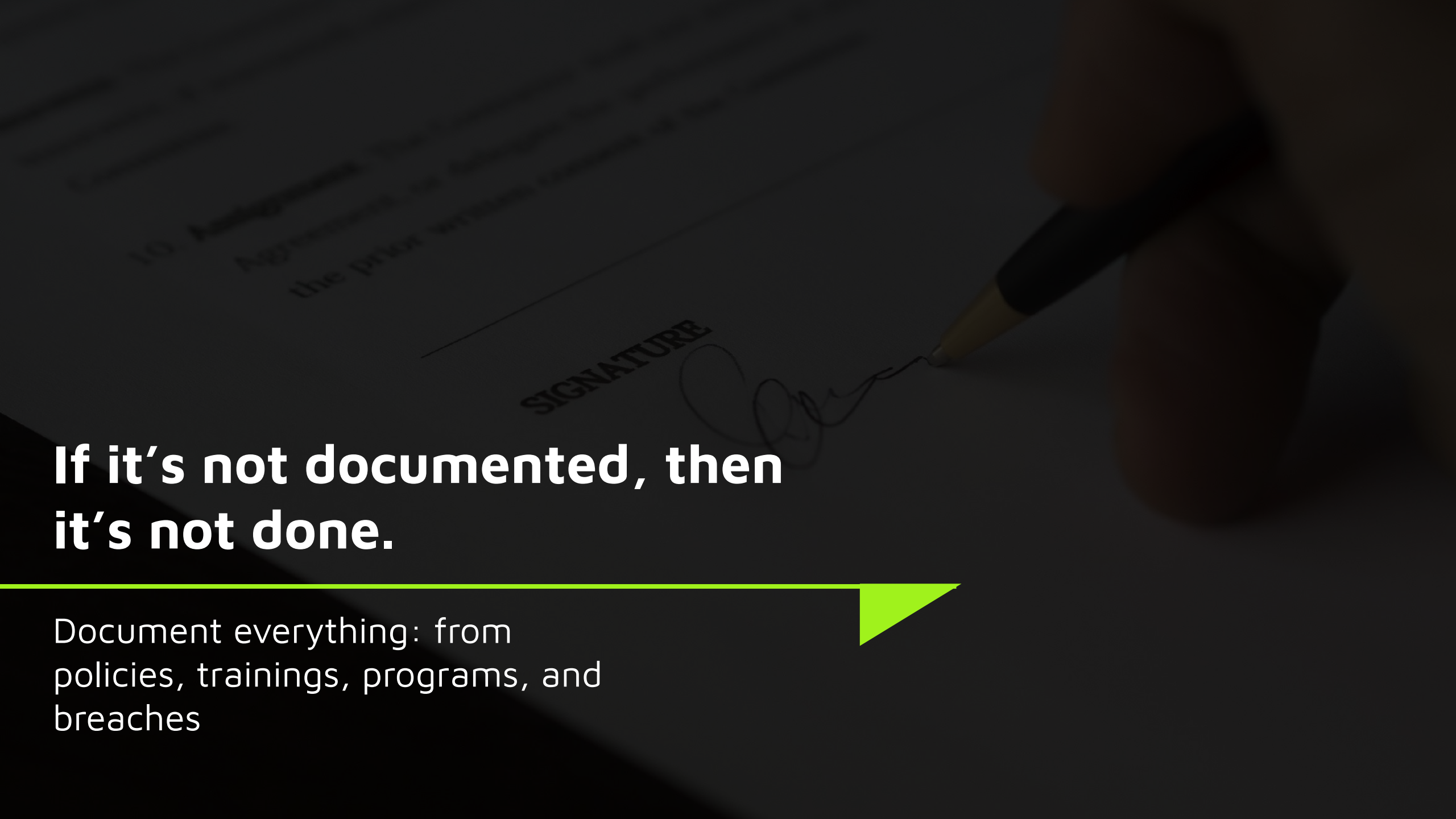
Executing and documenting HIPAA trainings

+

Responding to breaches immediately

+

Timely reporting of breaches

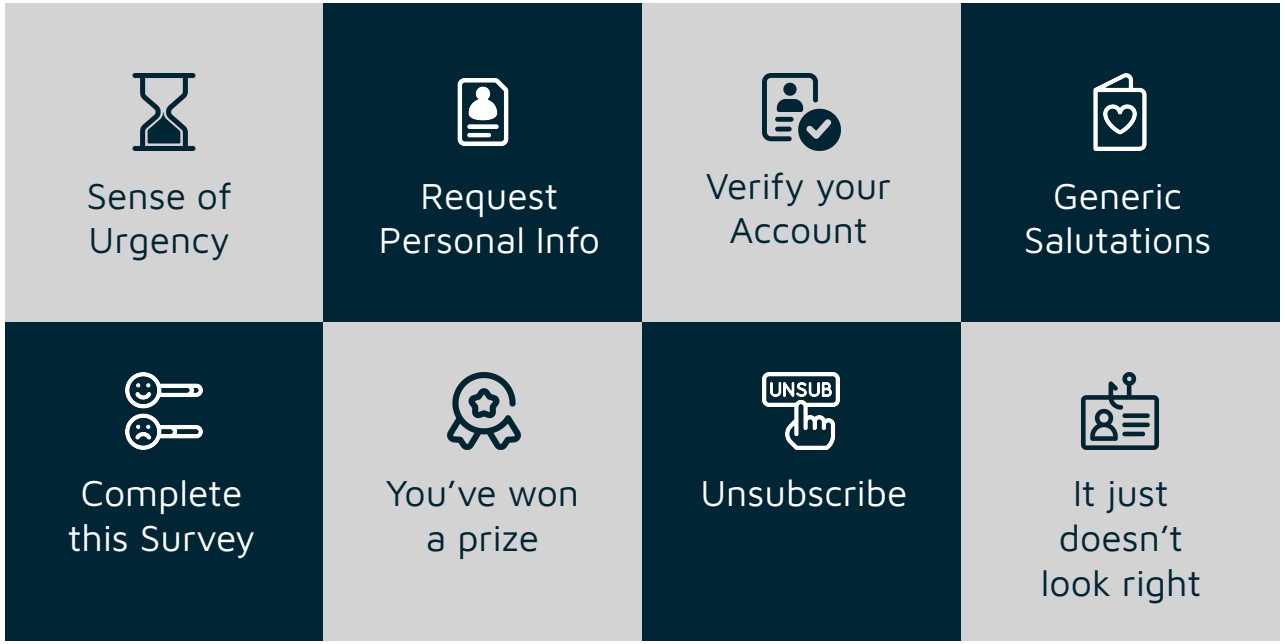


If it’s not documented, then it’s not done.

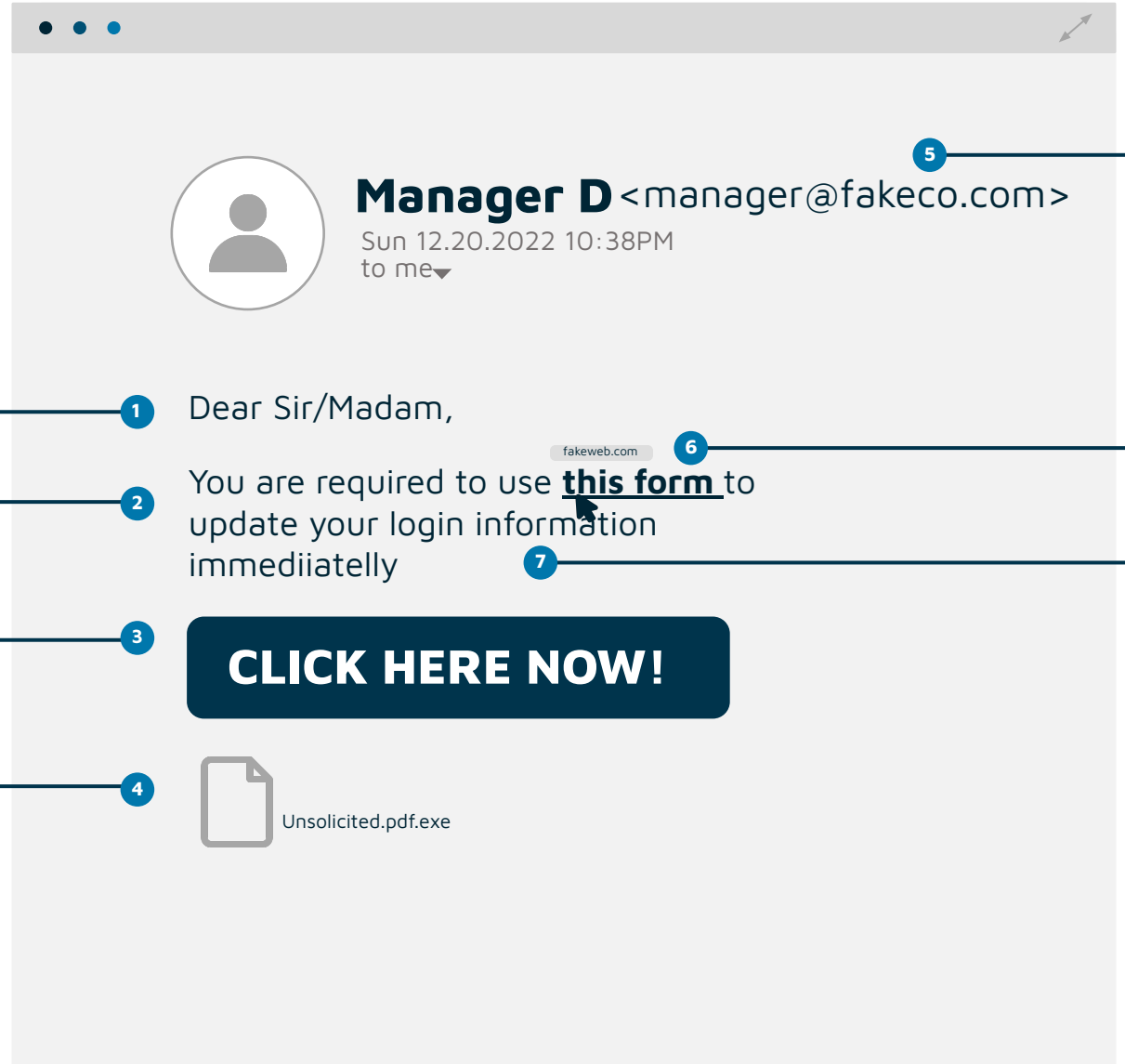
Document everything: from policies, trainings, programs, and breaches

LEARNING TO SPOT PHISHING EMAILS

Phishing emails are designed to trick you to reveal your personal information to cybercriminals by posing as a legitimate email.

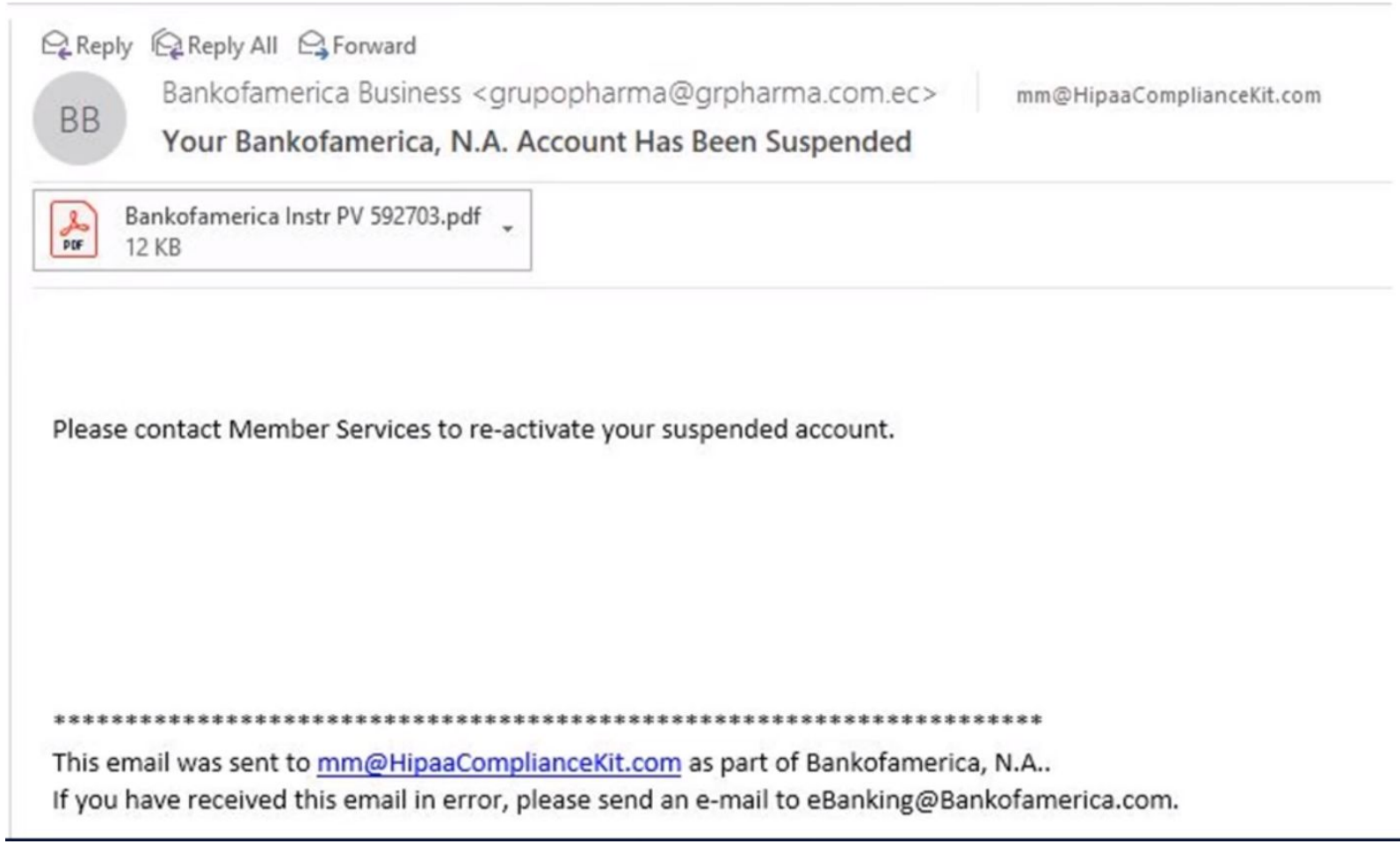


SIGNS OF A PHISHING EMAIL



1. Generic greeting or no greeting at all
2. Request for personal information over email
3. Buttons with hyperlinks to unfamiliar webpages
4. Unsolicited attachments
5. "From" email address is not official address
6. Hover your mouse to reveal misleading URL hyperlinks
7. Spelling and grammar mistakes

“PHISHY” EMAIL ADDRESSES



Reply Reply All Forward

BB

Bankofamerica Business <grupopharma@grpharma.com.ec>

mm@HipaaComplianceKit.com

Your Bankofamerica, N.A. Account Has Been Suspended

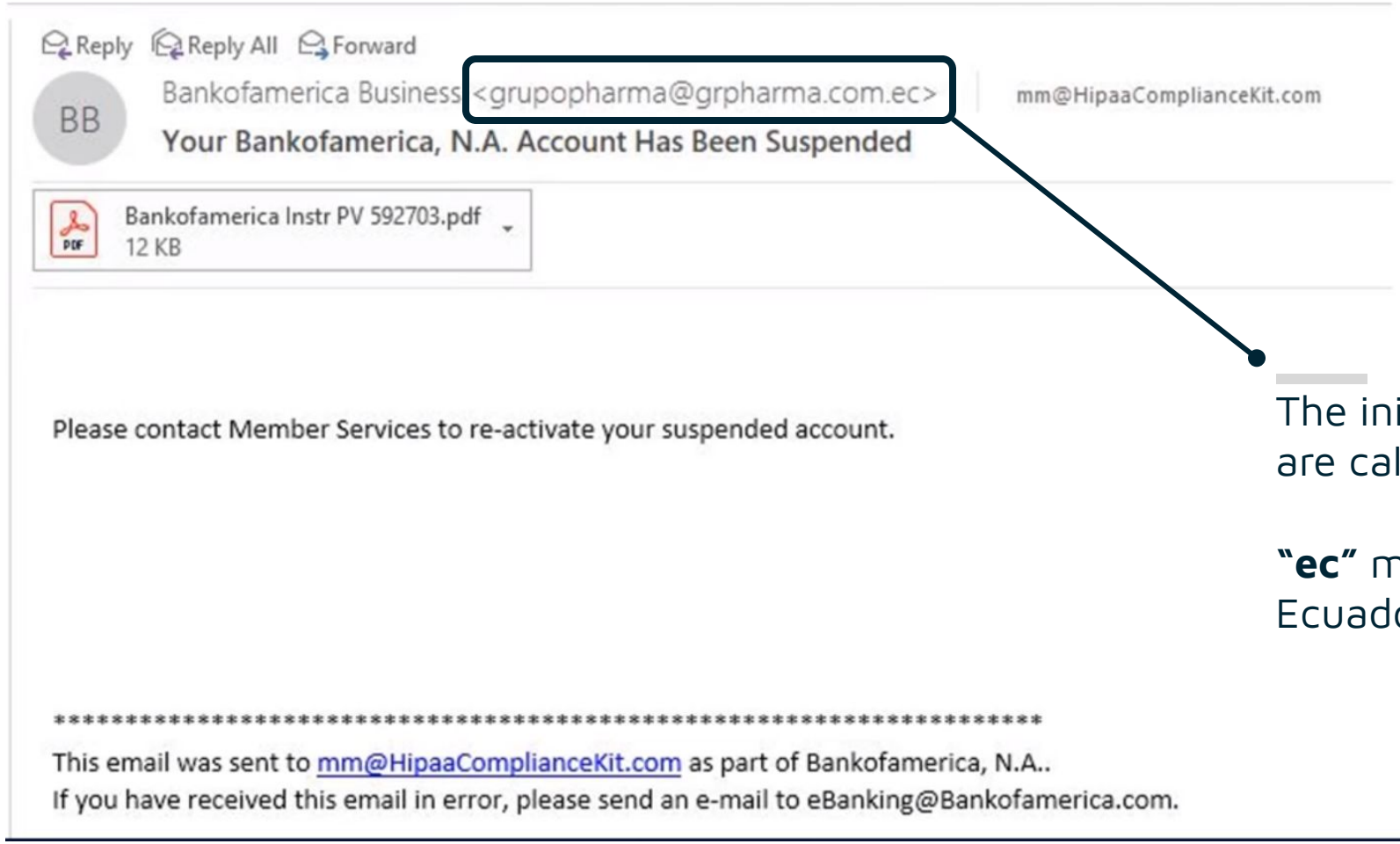
Bankofamerica Instr PV 592703.pdf
12 KB

Please contact Member Services to re-activate your suspended account.

****

This email was sent to mm@HipaaComplianceKit.com as part of Bankofamerica, N.A..
If you have received this email in error, please send an e-mail to eBanking@Bankofamerica.com.

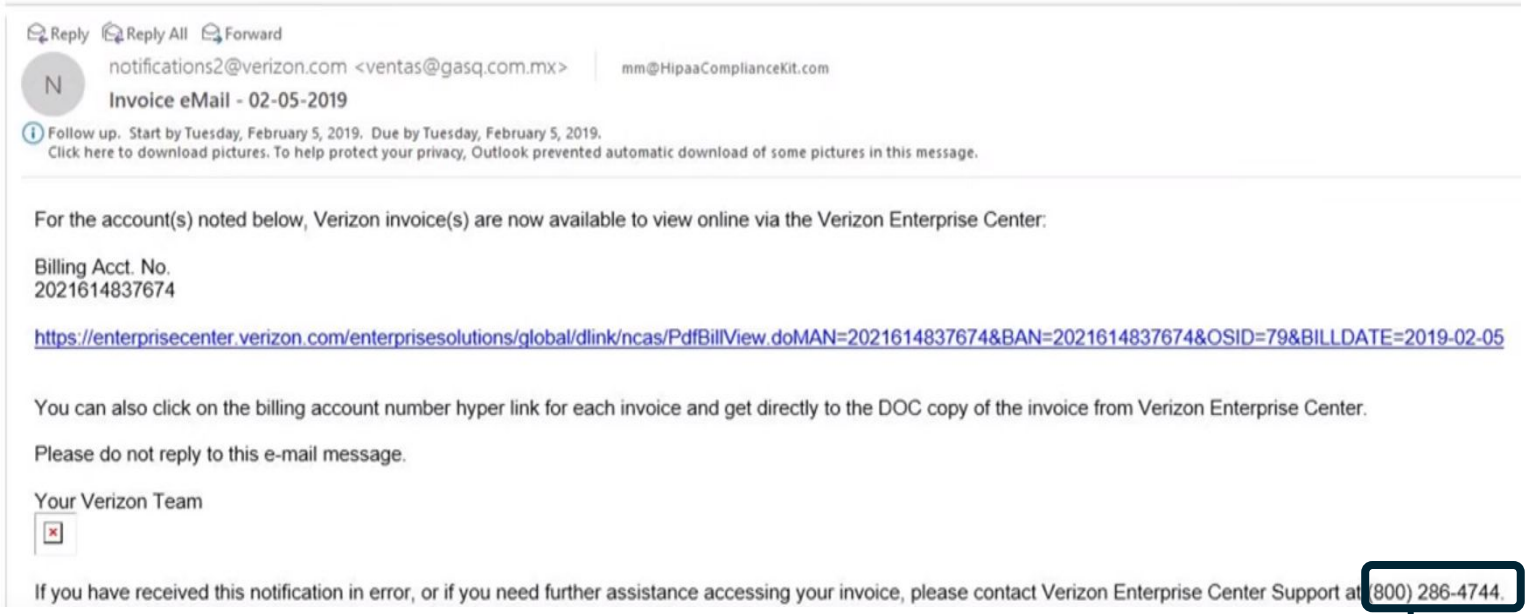
"PHISHY" EMAIL ADDRESSES



The initials after .com or .net are called a **country code.**

"ec" means the email is from Ecuador.

ADDING CUSTOMER SUPPORT NUMBERS



Reply Reply All Forward

N notifications2@verizon.com <ventas@gasq.com.mx> mm@HipaaComplianceKit.com

Invoice eMail - 02-05-2019

Follow up. Start by Tuesday, February 5, 2019. Due by Tuesday, February 5, 2019.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

For the account(s) noted below, Verizon invoice(s) are now available to view online via the Verizon Enterprise Center:

Billing Acct. No.
2021614837674

https://enterprisecenter.verizon.com/enterprisesolutions/global/dlink/ncas/PdfBillView.doMAN=2021614837674&BAN=2021614837674&OSID=79&BILLDATE=2019-02-05

You can also click on the billing account number hyper link for each invoice and get directly to the DOC copy of the invoice from Verizon Enterprise Center.

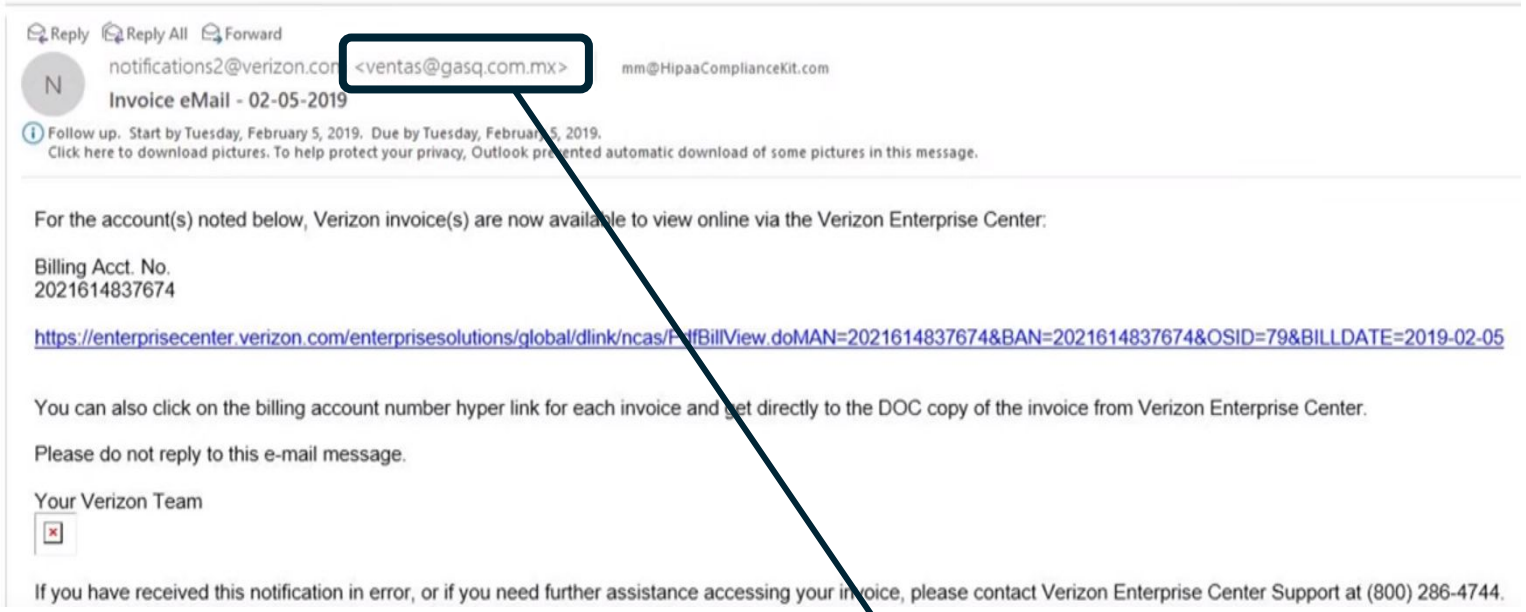
Please do not reply to this e-mail message.

Your Verizon Team

If you have received this notification in error, or if you need further assistance accessing your invoice, please contact Verizon Enterprise Center Support at (800) 286-4744.

Most phishing emails add an invalid support number to appear more legitimate

ADDING CUSTOMER SUPPORT NUMBERS



Reply Reply All Forward

N notifications2@verizon.com <ventas@gasq.com.mx> mm@HipaaComplianceKit.com

Invoice eMail - 02-05-2019

Follow up. Start by Tuesday, February 5, 2019. Due by Tuesday, February 5, 2019.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

For the account(s) noted below, Verizon invoice(s) are now available to view online via the Verizon Enterprise Center:

Billing Acct. No.
2021614837674

https://enterprisecenter.verizon.com/enterprisesolutions/global/dlink/ncas/PdfBillView.doMAN=2021614837674&BAN=2021614837674&OSID=79&BILLDATE=2019-02-05

You can also click on the billing account number hyper link for each invoice and get directly to the DOC copy of the invoice from Verizon Enterprise Center.

Please do not reply to this e-mail message.

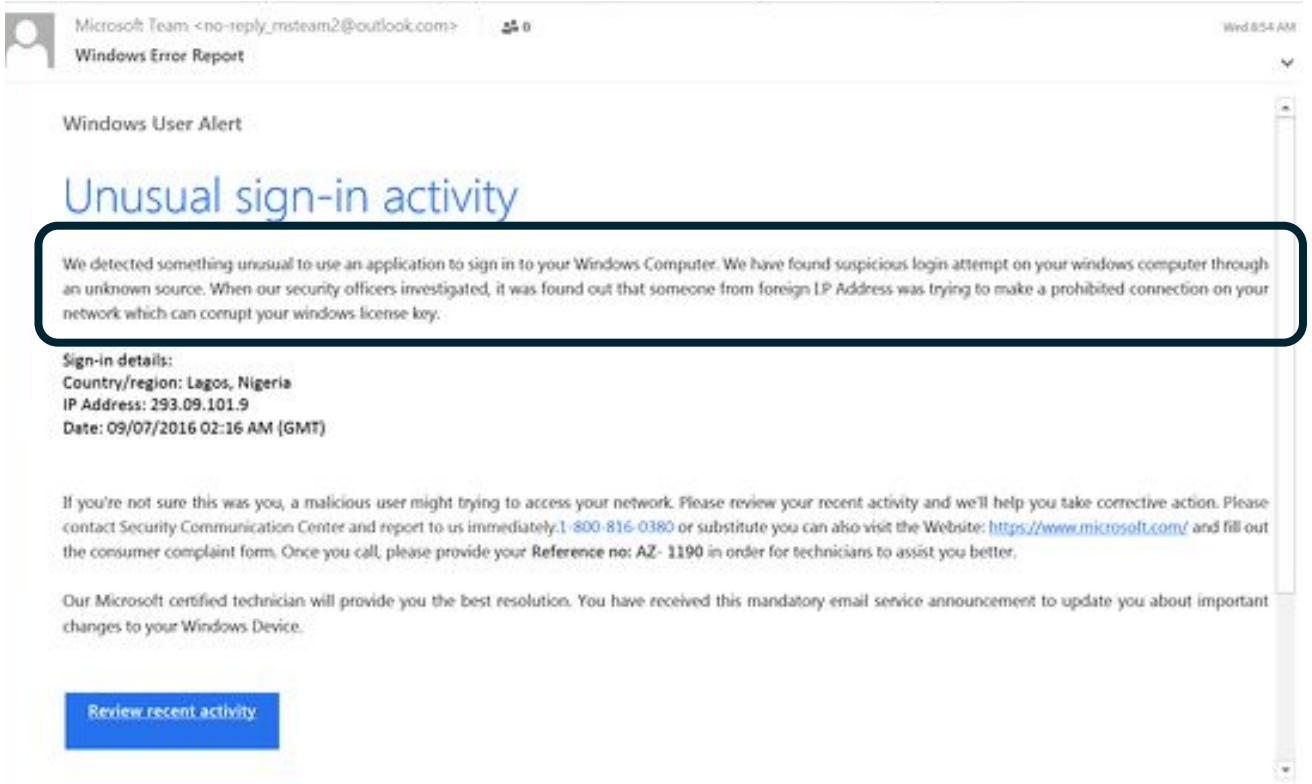
Your Verizon Team

If you have received this notification in error, or if you need further assistance accessing your invoice, please contact Verizon Enterprise Center Support at (800) 286-4744.

Again check the sender's address. This email is NOT going to Verizon.

More than that, it's being redirected to Mexico.

POORLY WRITTEN EMAILS



Microsoft Team <no-reply_msteam2@outlook.com> 0 Wed 8:54 AM

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 I.P 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)

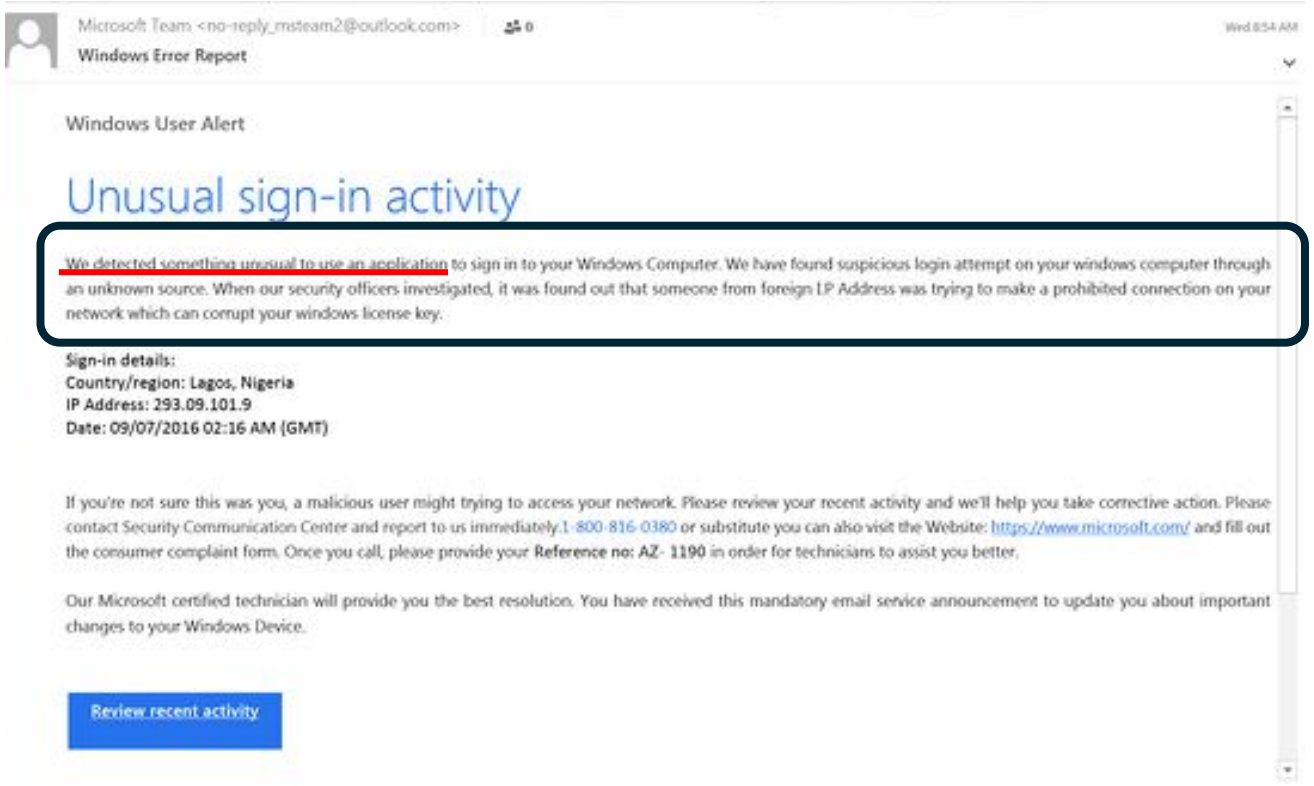
If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ 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

Cybercriminals often use a spellchecker and translation machine, giving them all the right words but not necessarily in the proper context.

POORLY WRITTEN EMAILS



Microsoft Team <no-reply_msteam2@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 I.P 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.1-800-816-0380 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.

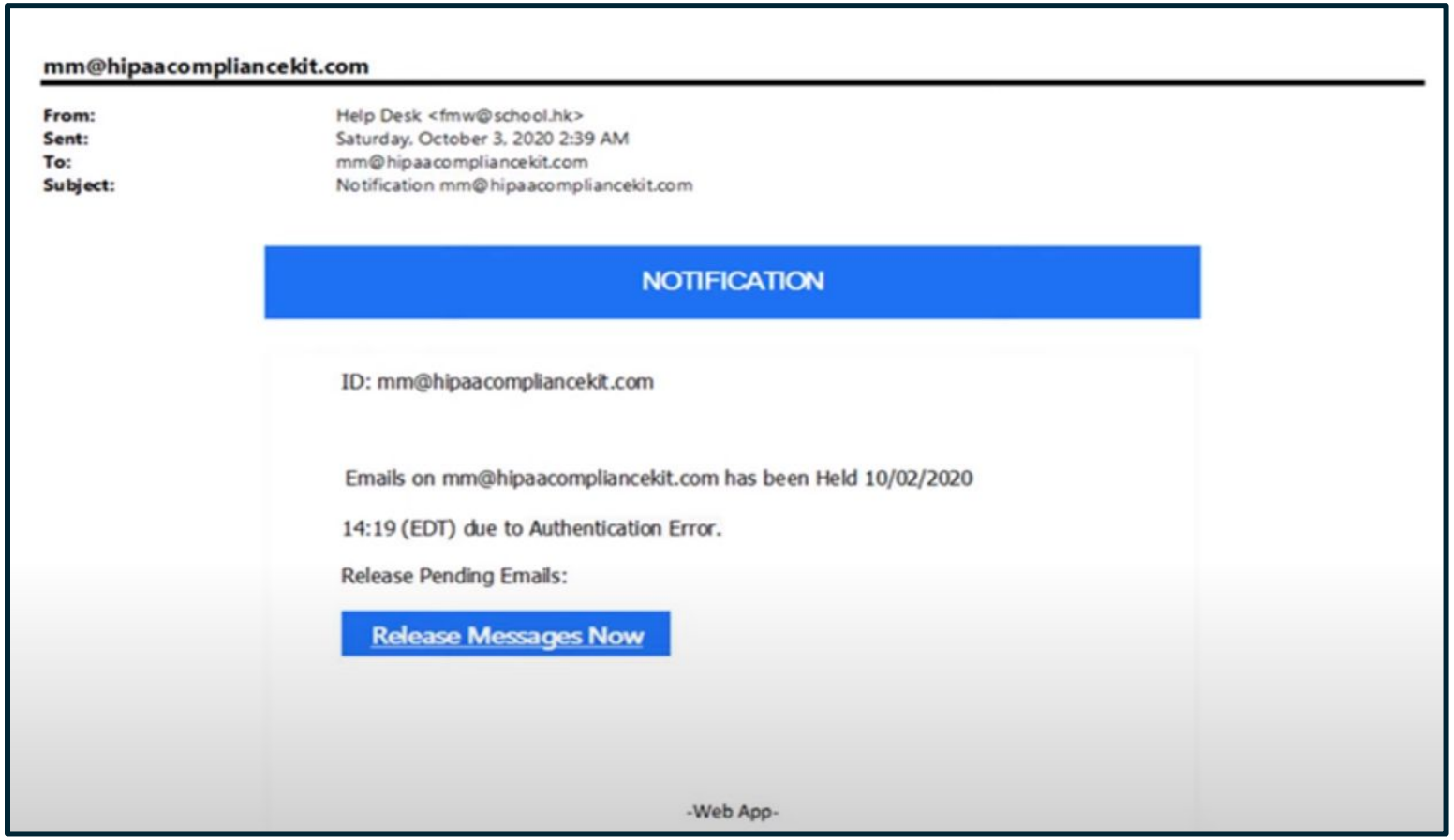
Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

Underlined phrase:
"We detected something unusual to use an application…"

In this phrase, no individual word is misspelled, but the message contains grammatical errors that a native or proficient speaker wouldn't make.

CREATING A SENSE OF URGENCY



Always consult the IT department when it comes to emails that appear to be urgent but are not sent from within the organization.

USING COMPLEX PASSWORDS

A complex password consists of:

At least
12
Alphanumeric characters

Aa
Upper and lower case letters

123
At least 2 numbers

@
At least 1 symbol

A firm was penalized
$600,000
for being responsible for a data breach due to having weak passwords

ENCRYPTING EMAILS

BOTH

Emails at Rest

Emails in Transit

SHOULD BE ENCRYPTED

WORK SHOULD BE LEFT AT WORK

CASE 1

Towards the end of the shift an implementer was not able to finish working on some patient visit notes for the day. Since this was a very important client, she needed to have them done before the next shift. She decided to send the visit notes to her personal email where she can finish working on them so as not to delay the client's workflow.

RESULT

WORK SHOULD BE LEFT AT WORK

CASE 1

Towards the end of the shift an implementer was not able to finish working on some patient visit notes for the day. Since this was a very important client, she needed to have them done before the next shift. She decided to send the visit notes to her personal email where she can finish working on them so as not to delay the client's workflow.

RESULT

FINAL WRITTEN WARNING

WORK SHOULD BE LEFT AT WORK

CASE 2

The training team was creating a customer service program and needed to understand the actual situations the employees were facing. They were given access to some call recordings of real patients, their real information, and real interaction with employees. This was a favorite topic for one of the trainers and he was excited to build the program around these recordings. He forwarded them to his personal email to make a perfect program to show the next day.

RESULT

WORK SHOULD BE LEFT AT WORK

CASE 2

The training team was creating a customer service program and needed to understand the actual situations the employees were facing. They were given access to some call recordings of real patients, their real information, and real interaction with employees. This was a favorite topic for one of the trainers and he was excited to build the program around these recordings. He forwarded them to his personal email to make a perfect program to show the next day.

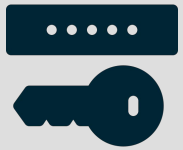
RESULT

TERMINATION

WORK SHOULD BE LEFT AT WORK

DO **NOT** FORWARD

Work emails



Work credentials

Work documents

TO YOUR PERSONAL EMAIL

OTHER THINGS TO REMEMBER

Activate two-factor authentication on your work email

OTHER THINGS TO REMEMBER

Activate two-factor authentication on your work email

Never share your passwords with colleagues unless authorized to do so

OTHER THINGS TO REMEMBER

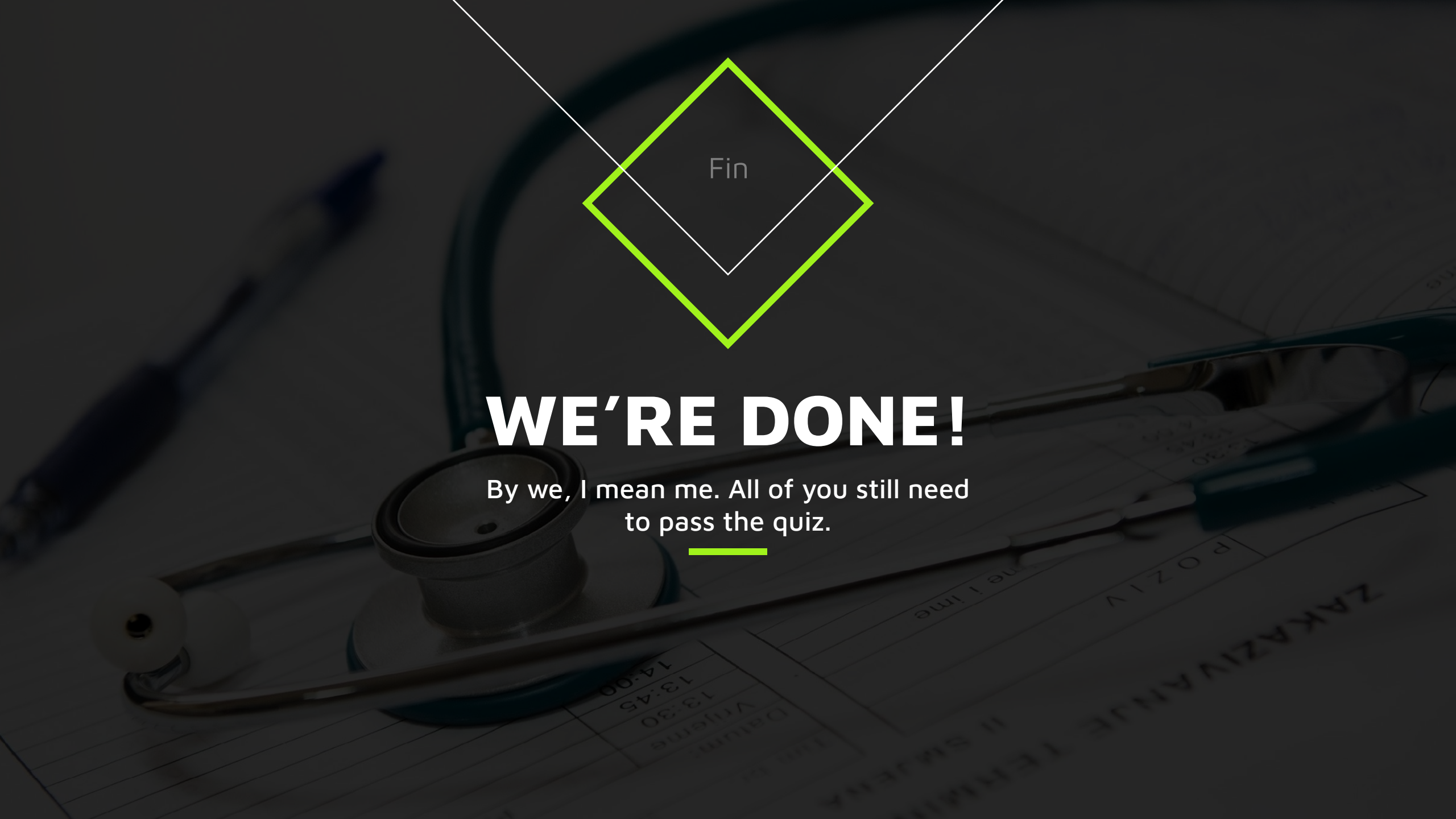
Activate two-factor authentication on your work email

Never share your passwords with colleagues unless authorized to do so

Lock your stations when you are away.

OTHER THINGS TO REMEMBER

How do you stay
HIPAA compliant?



WE'RE DONE!

By we, I mean me. All of you still need to pass the quiz.

YES, THERE'S AN EXAM

and it's mandatory.

Description

This is a mandatory course for all employees to undergo and get certifie d..

Course Content

HIPAA Resources

HIPAA Certification 2022