

Cybersecurity



Protect yourself from the bad guys!

Instructor Ben Vivante

ben@vivante.us

617-249-4197

www.vivante.us

What do the bad guys want from me?

- Your money
- Your presence on other sites
- Your Personal Identifiable Information (PII)
 - Full Name
 - Social Security #
 - Date of Birth
 - Gender
 - Mother Maiden Name
 - and much more
- In some cases to just exploit vulnerabilities on your computer.



Email Security

Some Basic Email Security Measures

- Don't use auto reply or out of office
- Limit identifying information in signatures
- Log in only on your computers
- Don't open unknown and strange emails
- Disable Images



Phishing Campaigns

Phishing Campaign and Spear Phishing

- Phishing scams are messages that try and trick you into providing sensitive information, often redirecting you with links to bad sites.
 - enter password
 - date of birth
 - confirm cc numbers
- Spear Phishing, email that appears to be from someone you know or uses Social Engineering target at you to get a certain result.



Don't get
hooked
by an
email
scam.

To ensure delivery, add onlinebanking@ealerts.bankofamerica.com to your address book.

Exclusively for: | [@udel.edu](#)



Online Banking Alert
Email Address Updated

Security Checkpoint:

You last signed in to Online Banking on 06/01/2012.
Remember: Always look for your SiteKey® before entering your Passcode.

Your primary email address was set up or changed on 06/01/2012.

Your security is important to us. If you did not authorize this change, please contact us immediately at [Click Here](#).

This Alert relates to your Online Banking profile, rather than a particular account. The account listed here is for verification purposes only.

Want to confirm this email is from Bank of America? Sign in to [Online Banking](#) and go to [Alerts](#). The Alerts History lists the Alerts sent to you in the past 60 days.

Like to get more Alerts? Sign in to your Online Banking account at Bank of America and within the Accounts Overview page select the Alerts tab.

Security Checkpoint: This email includes a Security Checkpoint. The information in this section lets you know this is an authentic communication from Bank of America. Remember to look for your SiteKey every time you sign in to Online Banking.

Email Preferences

This is a service email from Bank of America. Please note that you may receive service email in accordance with your Bank of America service agreements, whether or not you elect to receive promotional email.


Contact us about this email

Please do not reply to this email with sensitive information, such as an account number, PIN, password, or Online ID. The security and confidentiality of your personal information is important to us. If you have any questions, please either call the phone number on your account statement or use the [Contact Us](#) page, so we can properly verify your identity.

Privacy and Security

Keeping your financial information secure is one of our most important responsibilities. For an explanation of how we manage customer information, please read our [Privacy Policy](#). You can also learn how Bank of America keeps your [personal information secure](#) and how you can help protect yourself.

Bank of America Email, 8th Floor-NC1-002-08-25, 101 South Tryon St., Charlotte, NC 28255-0001

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#) 
© 2012 Bank of America Corporation. All rights reserved.

This email was sent to: [@udel.edu](#)

Phish leading to Imposter Site

Security error x Security error x Bank of America

sclgchl1.eu.pn/index3.html

Bank of America Secure Area

Confirm Your Information

To Verify your Identity, please enter the following.

Your complete account number
Ensure you input your Correct Account Number.
Numbers only

Your complete Social Security number (SSN) or Tax Identification number (TIN)
Input Correct Numbers

Your Passcode

Reminder: Your payment declined!



cpanel-...,y.txt

email-m...,mobileconfig

email-i...,mobileconfig



Your payment didn't go through

We regret to inform you that the payment method submitted for the forthcoming month has been unfortunately declined. To ensure uninterrupted access to our services and avoid any potential downgrade in service quality, we kindly request that you update your payment details at your earliest convenience.

[Manage payments](#)

Remember, you can view your payment history or change your payment method at any time in the Billing section of your [Xfinity](#) account.

This is a service-related email to keep you informed about your [Xfinity](#) account. Please do not reply to this email; it is not monitored.

Comcast respects your privacy. For a complete description of our privacy policy,

[Xfinity](#) Customer Agreements, Policies and Service Disclosures

Device Payment Plan Agreement

For our [Xfinity](#) return policy, click here.

© Comcast. All rights reserved.


All trademarks are the property of their respective owners.

[Xfinity](#)

1701 JFK Boulevard, Philadelphia, PA 19103

Attn: Email Communications

Examples of Phishing Emails

 Thu 10/20/2016 3:20 PM
American Express <AmericanExpress@aexpress.com>
Payment is past due

To Ben Vivante
[Retention Policy](#) [Junk Email \(30 days\)](#)

[Action Items](#)

Your payment is past due

Dear Cardholder,

The payment date for your Business Gold Rewards Card account is now passed.

Statement Balance:	\$6309.73
Payment Due:	\$6309.73

If you have already sent or scheduled your payment, please [Contact us here](#).

[Make a payment](#) [View recent activity](#) [Update alert settings](#)


Thank you for your Cardmembership.

Sincerely,
American Express Customer Service

The linke d i...

For your security:

The lin...



TEXT AND RECEIVE

Enroll in Text MYAMEX and have account information texted to you on request.
Carrier charges may apply for receiving and sending text messages.

ENROLL NOW



Thu 10/20/2016 3:28 PM

American Express Alerts <alerts@americanexpress.co>

Large Purchase Made

To Ben Vivante

[Retention Policy](#) [Junk Email \(30 days\)](#)

[Expires](#) [Never](#)



Hello, Ben Vivante

Account Ending:
**005



[View Account](#)

[Make a Payment](#)

[Manage Alerts Preferences](#)



The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.



Th **Large Purchase**

[View Account](#)

The following purchase was above the notification amount you set for your account.


Notification Amount:	\$1,000.00
Transaction Time:	9:35 AM
Merchant Name:	FERRARI
Purchase Amount:	\$8,000.00

Some transactions are pre-authorized before the final sale. These can include purchases made at gas stations, hotels, and car rental merchants. Please note the amount shown above may not reflect the exact amount of your final transaction.

See something you don't recognize? [Log into](#) your account and mark the pending charge in your recent charges. We'll monitor this transaction and let you know when it posts to your account.

Close

POURSUITE JUDICIAIRE du 03/003/2023

 Translate message to: English | Never translate from: French



Gendarmerie Nationale <ngendarmerie58@gmail.com>

To: garde.nationale-gendarmerie31@france1.fr



DGD33 (4) (8).pdf



Bonjour

Merci de prendre connaissance du document en pièce jointe et
Nous contactez le plus rapidement.
Cordialement,

Gendarmerie Nationale

 Reply

 Forward



Coinbase <no-reply@statalab.com>

To: You

coinbase

You successfully completed ID verification.

If this wasn't you, lock your account immediately and change your password.

[Lock my account](#)

© Coinbase 2023 | Coinbase Inc.
248 3rd St #434 | Oakland CA 94607 | US
(888) 908-7930



Thu 10/20/2016 3:28 PM

Groupon@grouponmail.net

75% Off iPad Mini at Apple Store LIMITED TIME

To Ben Vivante

[Retention Policy](#) [Junk Email \(30 days\)](#)

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

[Your Daily Groupon](#) | [Go to Groupon](#) |



The Daily Deal for
Groupon Users

follow us:

iPad Mini limited quantities!

\$99!

See Today's Deal

worth: discount: savings:

\$399 75% \$300

Company Information:

Apple
Online Only at Apple Store

Locations:
Apple Store Online



www.vivante.us



Thu 10/20/2016 3:28 PM

Groupon@grouponmail.net

75% Off iPad Mini at Apple Store LIMITED TIME

To Ben Vivante

[Retention Policy](#) [Junk Email \(30 days\)](#)

[i](#) If there are problems with how this message is displayed, click here to view it in a web browser.

[Your Daily Groupon](#) | [Go to Groupon](#) |



The Daily Deal for
Groupon Users

follow us: [f](#) [t](#)

iPad Mini limited quantities!

\$99!

See Today's Deal

worth: discount: savings:

\$399 75% \$300

Company Information:

Apple
Online Only at Apple Store

Locations:
Apple Store Online



www.vivante.us

From: Jordan Williams <jordan@mypensionassistance.com>

Subject: UC Santa Cruz Annual Pension Review

Date: Nov 4, 2022

To:

UC Santa Cruz Annual Pension Review

<Redacted Name>,

Title: Department Manager, <Redacted Name>

Department: <Redacted Name> Department

It's that time of the year again to schedule a one-on-one consultation regarding your specific state, federal, and individual retirement benefit questions.

At the meeting you'll learn what you can expect from UCRP when you retire, and how much longer you will need to work to maximize those benefits. You'll also receive advice on the best ways to utilize your 403(b) and 457(b) options with your UCRP and/or Social Security benefits, as well as get answers to general retirement questions.

Appointments are held over phone or by virtual meeting. To secure your spot, use the link below.

[Create Appointment](#)

Or visit: mypensionassistance.com

All licensed representatives are not employees of the school, state or the UCRP pension programs.

See [Privacy Policy](#) for more details about how we use your information.



Thu 10/20/2016 3:30 PM

My Flowers Online <Deliveries@MyFlowersOnline.net>

Flowers Could Not Be Delivered

> Ben Vivante

[Attention Policy](#) [Junk Email \(30 days\)](#)

Please do not reply to this email as it was sent from a notification-only address that cannot accept incoming emails.

Order Confirmation

Dear Recipient,

A gift was scheduled to be delivered to you today but there were errors in the delivery information.

Here are the details of the order:

Your Gift(s):



**Your Card
Message:**

I can't stop
thinking about
you...
Love, You
Know Who ;)



Thu 10/20/2016 3:30 PM

AccountUpdates@facebook-updates.com

Monthly Fee for Facebook Users

To Ben Vivante

[Retention Policy](#) [Junk Email \(30 days\)](#)

[Expires](#) [Never](#)

Dear Facebook User:

In an effort to make Facebook a safer and more secure social place, we have decided that at the end of this month we must begin charging a monthly fee for accessing our [site](#).

We have come to this conclusion for several reasons:

- Too many free accounts are being created for illegal purposes
- Our servers cannot handle the increased activity
- Our company has become publicly traded, and we're trying to increase our overall revenue

If you wish for Facebook to remain a free service, we are requiring all users sign a petition here:

[http://facebook.com/petition to remain free/fb id?9923820](http://facebook.com/petition%20to%20remain%20free/fb_id?9923820)

By signing the petition your account will remain free no matter what.

In order to ensure that your account remains on the free list, please sign the petition as soon as possible. There are only 10,000 spots available as free accounts.

Please do not reply to this email

Recap - Red Flags in Email

FROM

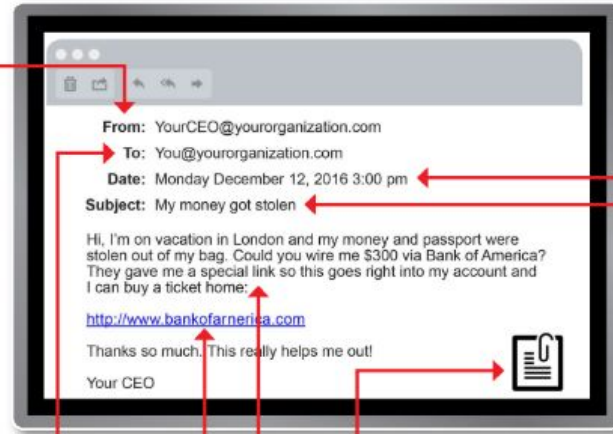
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner 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.bankofamerica.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?

Social Media Security



You Are the Product!



Facebook Basic Security

- Review your Privacy Settings
- Never Provide Correct Date of Birth
- Review Facebook Settings
- Don't make friends with people that aren't friends
- You can message without being friends
- REVIEW YOUR SECURITY SETTINGS

Think Before you Share



**THINK BEFORE
YOU SHARE**

Malware/Ransomware



- **Malware**

short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

- **Ransomware**

Ransomware is computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransom payment to decrypt it or not publish it.

Ransomware



•What does ransomware do?

- There are different types of ransomware. However, all of them will prevent you from using your PC normally, and they will all ask you to do something before you can use your PC.
- They can target any PC users, whether it's a home computer, endpoints in an enterprise network, or servers used by a government agency or healthcare provider.

•Ransomware can:

Prevent you from accessing Windows.

- Encrypt files so you can't use them.
- Stop certain apps from running (like your web browser).
- Ransomware will demand that you pay money (a “ransom”) to get access to your PC or files. We have also seen them make you complete surveys.
- There is no guarantee that paying the fine or doing what the ransomware tells you will give access to your PC or files again.

Ransomware Example

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)


Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



[REDACTED]


OK

Anti-Virus Software

- Some Basics:
 - Should be running all the time
 - Need to check that it's getting updates and scanning normally.
 - Not a bad idea to start your own scan
 - Have a professional Check your computer

Types of Anti-Virus Software

 **Best Overall**
Bitdefender Antivirus Plus


 **Best for Extra Security Features**
Norton AntiVirus Plus

 **Best for Single-PC Households**
McAfee AntiVirus

 **Best for Speedy Scans**
Malwarebytes Premium Security

 **Best for Thrifty Users**
Sophos Home Premium

 **Best for a Small Footprint**
Webroot Essentials

 **Best Breadth of Features**
G Data Antivirus

Consider AVG Antivirus - Free

Backup Strategies

- Store your important information in more than one place!
- Use Secure Clouds:
 - Google
 - Windows 365
 - Amazon
- Be careful with Detached Storage



Wireless Security

- Insecure by Nature
- Uses Radio Signal between router and your devices. Anyone within Distance of the radio signal may have access to the network. You can sometimes see your neighbors wireless networks. Anyone walking or riding by your house can likely see your wireless network, and can attempt to hack it.
- Use **WPA2** (Wireless Protected Access 2) with Strong Passwords

Check your Wireless Router Settings

verizon

Main Wireless Settings My Network Firewall Settings Parental Control Advanced System Monitoring

My Router

Router Status
GO!
Your Router is Ready for Internet Access

Broadband Connection

Ethernet Status: Connected
Connection Type: DHCP
IP Address: 98.113.85.179

Quick Links

- [Port Forwarding](#)
(Enable Applications: Games, IM & Others)
- [Change Wireless Settings](#)
- [Change Login User Name / Password](#)
- [Adding a Webcam](#)
- [Verizon Help](#)
- [Logout](#)

My Network

PC Name:	Bunny-PC
Connection Type:	Ethernet
IP Address:	192.168.1.2
Status:	Active
PC Name:	new-host-2
Connection Type:	Ethernet
IP Address:	192.168.1.3
Status:	Inactive
PC Name:	192.168.1.11
Connection Type:	Ethernet
IP Address:	192.168.1.11
Status:	Active

Action Zone

GO TO THE INTERNET NOW >

verizon

- [Verizon.com](#)
- [Verizon Central](#)
- [Verizon Business Center](#)
- [Verizon Surround](#)

Shop Actiontec >

Music >

Videos >

www.vivante.us

Avoid Public WiFi



Tips To Protect Yourself On Public WiFi

- 1 Keep an eye out for fake public hotspots or "rogue hotspots."
- 2 Never visit websites with personal information
- 3 Only visit secure "HTTPS" websites
- 4 Level up the security settings on your mobile devices
- 5 Use a VPN
- 6 Use anti-malware or antivirus protection for your devices
- 7 Log out of websites when done



Personal Cyber Security Best Practices

- Strong Password
 - new, unfamiliar, unrelated, 15 characters
- Don't let people look over your shoulder when entering passwords
- If you store credentials digitally, don't label them "User Name" or "Password" or "pw", these are the first things hackers will search for on your computer.
- Looks for 2 factor authentication, especially for financial information.
- Use unknown computer login email reminders.
- Use Card Not Present transaction notifications from banks and cc companies.
- Avoid online banking or secure transactions on mobile devices and any keyboard that's not your own.
- Don't use open wireless networks

Mobile security

INFOSEC

What is mobile security?

Mobile security refers to cybersecurity on mobile computing devices. This has become much more common in recent years, thanks in part to the popularity of smartphones. One source estimates that 24,000 malicious apps are blocked every day.

So this is about my phone?

Yes, but not just your phone. Laptops, tablets and even smart home devices need mobile security.



What's the biggest threat to a mobile device?

Malware is definitely a major problem for mobile devices. Many people don't realize that phones and tablets can get malware. People downloading apps and games open themselves to catching computer viruses.



Download on the
App Store

There's this cool security app I can download ...

Hold the phone! (Well, you already were, but you know what we mean.) Examine that app carefully before you download it and make sure you're getting it from the official app store.

What about antivirus software for mobile devices?

It's out there and available from reliable providers on all mobile platforms. Check it out. You won't regret it!



Can I password-protect a phone?

Absolutely! Check your phone's settings menu. For a double dose of security, implement encryption as well. (See below!)



What's one thing I can do to improve mobile security?

Encrypt your device. An encrypted device is unreadable to someone without the password, even if they take it apart to physically extract the chip. You can enable device encryption in your device's settings menu.



20 Ways to Block Mobile Attacks

Don't let your guard down just because you're on a mobile device. Be just as careful as you would on a desktop!

WiFi

- Don't allow your device to auto-join unfamiliar networks.
- Always turn off WiFi when you aren't using it or don't need it.
- Never send sensitive information over WiFi unless you're absolutely sure it's a secure network.

Apps

- Only use apps available in your device's official store - NEVER download from a browser.
- Be wary of apps from unknown developers or those with limited/bad reviews.
- Keep them updated to ensure they have the latest security.
- If they're no longer supported by your store, just delete!
- Don't grant administrator, or excessive privileges to apps unless you truly trust them.

Browser

- Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that appear to be legit.
- Pay close attention to URLs. These are harder to verify on mobile screens but it's worth the effort.
- Never save your login information when you're using a web browser.



Bluetooth

- Disable automatic Bluetooth pairing.
- Always turn it off when you don't need it.

Smishing (phishing via SMS)

- Don't trust messages that attempt to get you to reveal any personal information
- Beware of similar tactics in platforms like What's App, Facebook Messenger Instagram, etc.
- Treat messages the same way you would treat email, always think before you click!

Vishing (voice phishing)

- Do not respond to telephone or email requests for personal financial information. If you are concerned, call the financial institution directly, using the phone number that appears on the back of your credit card or on your monthly statement.
- Never click on a link in an unsolicited commercial email.
- Speak only with live people when providing account information, and **only** when you initiate the call.
- Install software that can tell you whether you are on a secure or fake website.