Cybersecurity Awareness Training

81% of organizations around the world have experienced an increase in email phishing attacks since March 2020, and a recent study by APWG observed a record number of phishing attacks in Q3 2022. But despite this..., almost 1 in 5 organizations only deliver phishing awareness training to their employees once per year.

- Expert Insights / IRONSCALES

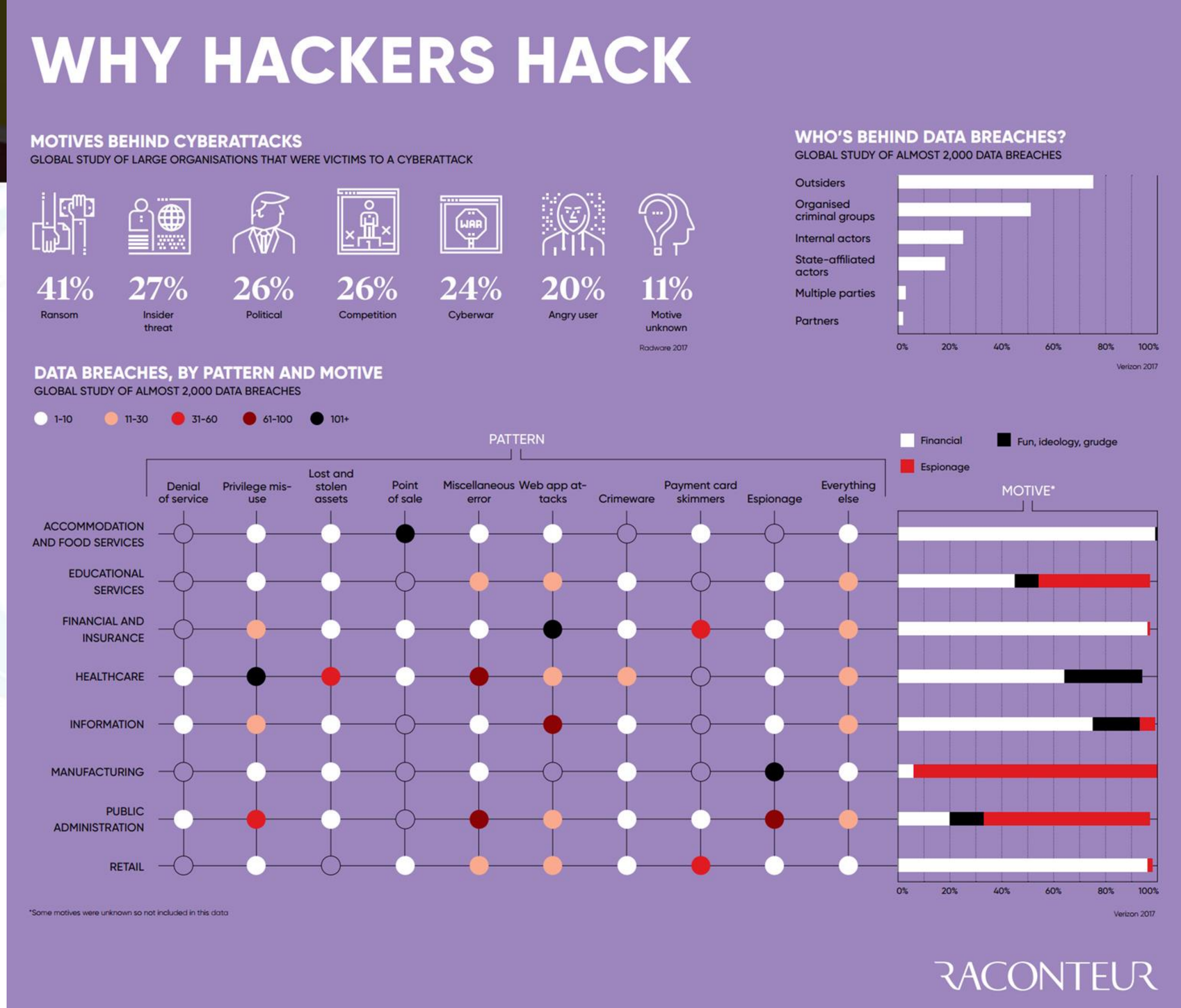
INTRODUCTION

Our Goals

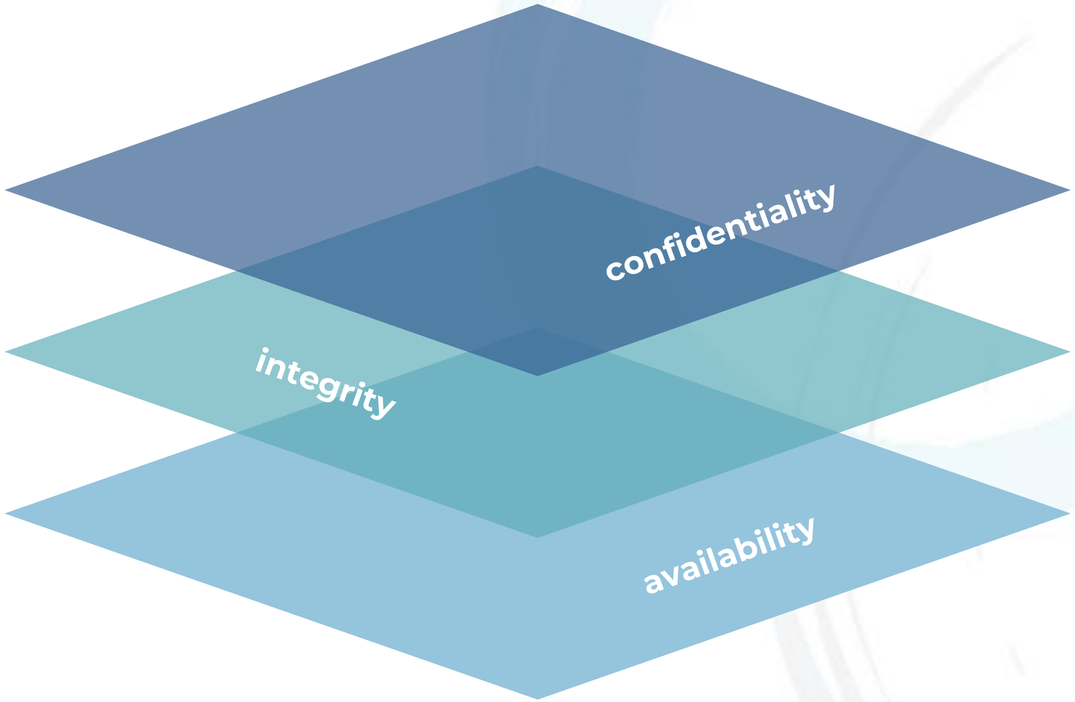
1. **Acquire knowledge** and understanding.
2. Learn how to **identify risks**.
3. Learn **best practices**.

Why Hackers Hack

+ Money
+ Power
+ Politics
+ Competition
+ Bragging Rights
+ Revenge
+ Unknown



Cybersecurity Objectives for Companies

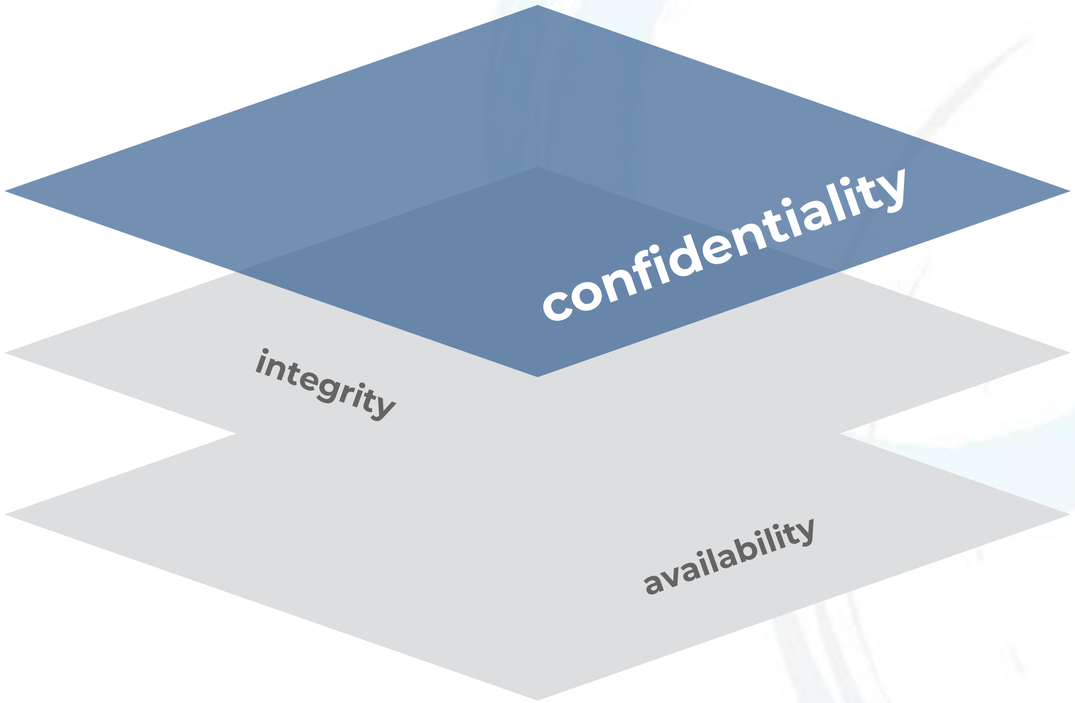


NIST Special Publication 800-12, revision 1
An Introduction to Information Security section 1.4

3 Cybersecurity Objectives For a Company:

1. Confidentiality
2. Integrity
3. Availability

Cybersecurity Objectives...



NIST Special Publication 800-12, revision 1
An Introduction to Information Security section 1.4

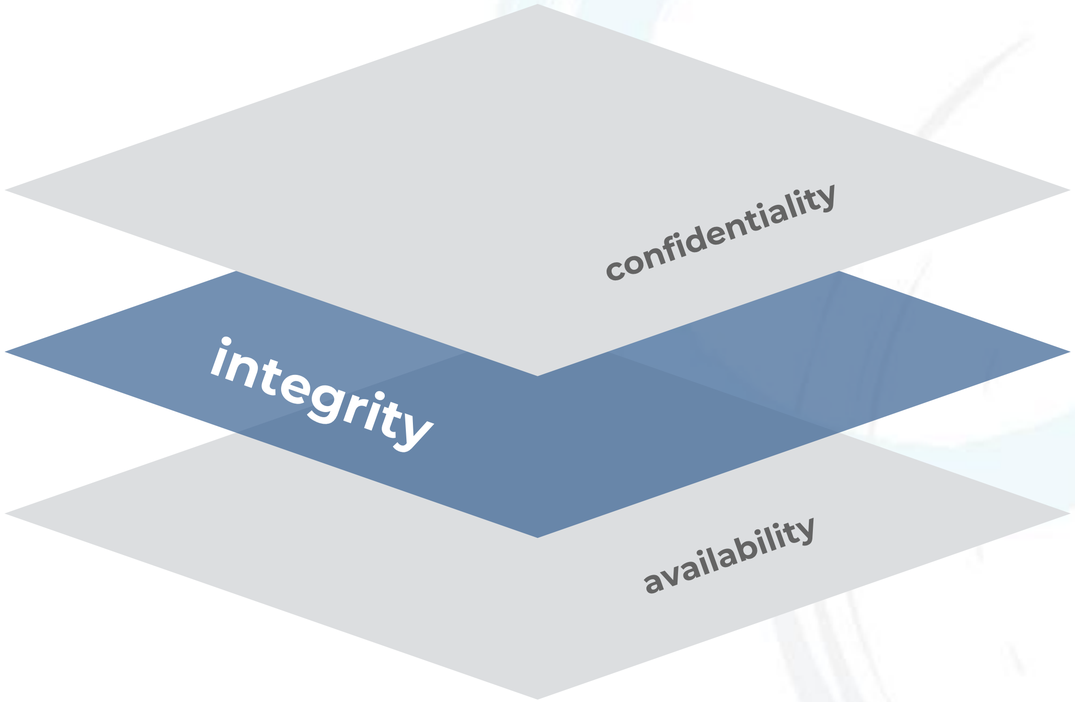
CONFIDENTIALITY

Protecting information from **unauthorized access** and disclosure...

Example:

Criminal steals customers' usernames, passwords, or credit card information.

Cybersecurity Objectives...



NIST Special Publication 800-12, revision 1
An Introduction to Information Security section 1.4

INTEGRITY

Protecting information from **unauthorized modification**...

Example:

Someone alters payroll information or a proposed product design.

Cybersecurity Objectives...

NIST Special Publication 800-12, revision 1
An Introduction to Information Security section 1.4

AVAILABILITY

Preventing disruption in how information is accessed...

Example:

Your customers are unable to access your online services.

Quiz Time!

FTC CyberSecurity Quiz

CYBERSECURITY THREATS

Overview

Why Should You Care?

1. Small businesses are a **good mark** these days.
2. The **costs** of a breach can be devastatingly high.
3. Your **reputation**, once damaged, is hard to rebuild.

Common Threats

1. **Phishing and ransomware** attacks.
2. **Malicious websites** and Social Media Phishing (“SMishing”).
3. **Social engineering**/Imposter Scams.
4. **Hacking** and Password Cracking.

Email Phishing

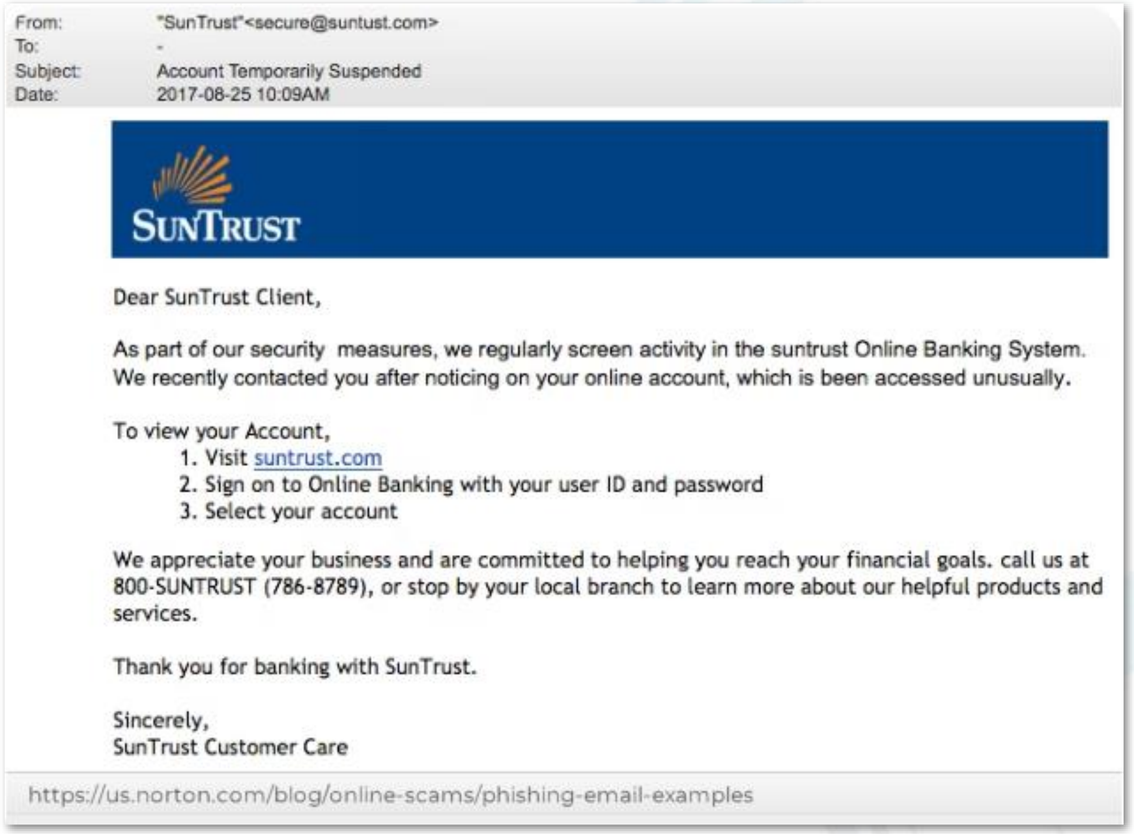
What is Phishing?

From the mighty Oxford Dictionary: *the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.* **Is this correct?** Methods might include email, texting, WhatsApp, social media apps, etc.

How to Spot an Attack AND Avoid Being Tricked

1. **Check the email address** and look for **sloppy layout** and/or **spelling and grammatical errors.**
2. **Check the greeting.** "Dear customer" or a generic greetings can be a give away.
3. **Look for spoofed hyperlinks** by hovering your mouse over the link to see if it is different from the destination displayed in the message.
4. **Treat all attachments and links with caution**!!!
5. **Be suspicious of any message** that requests you to click a link or open an attachment!!!
6. **Beware messages promoting a sense of urgency** or dire consequences if you don't act immediately.
7. **Contact the person or the organization** using a different, validated method like a phone number you already know OR look up the organization's website 'Contact Us' information. Never use the message's links or contact information!!!
8. **Do not provide personal or sensitive information** in response to a message.

Email Phishing... Oh My!



From: "SunTrust"<secure@suntust.com>
To: -
Subject: Account Temporarily Suspended
Date: 2017-08-25 10:09AM

SUNTRUST

Dear SunTrust Client,

As part of our security measures, we regularly screen activity in the suntrust Online Banking System. We recently contacted you after noticing on your online account, which is been accessed unusually.

To view your Account,

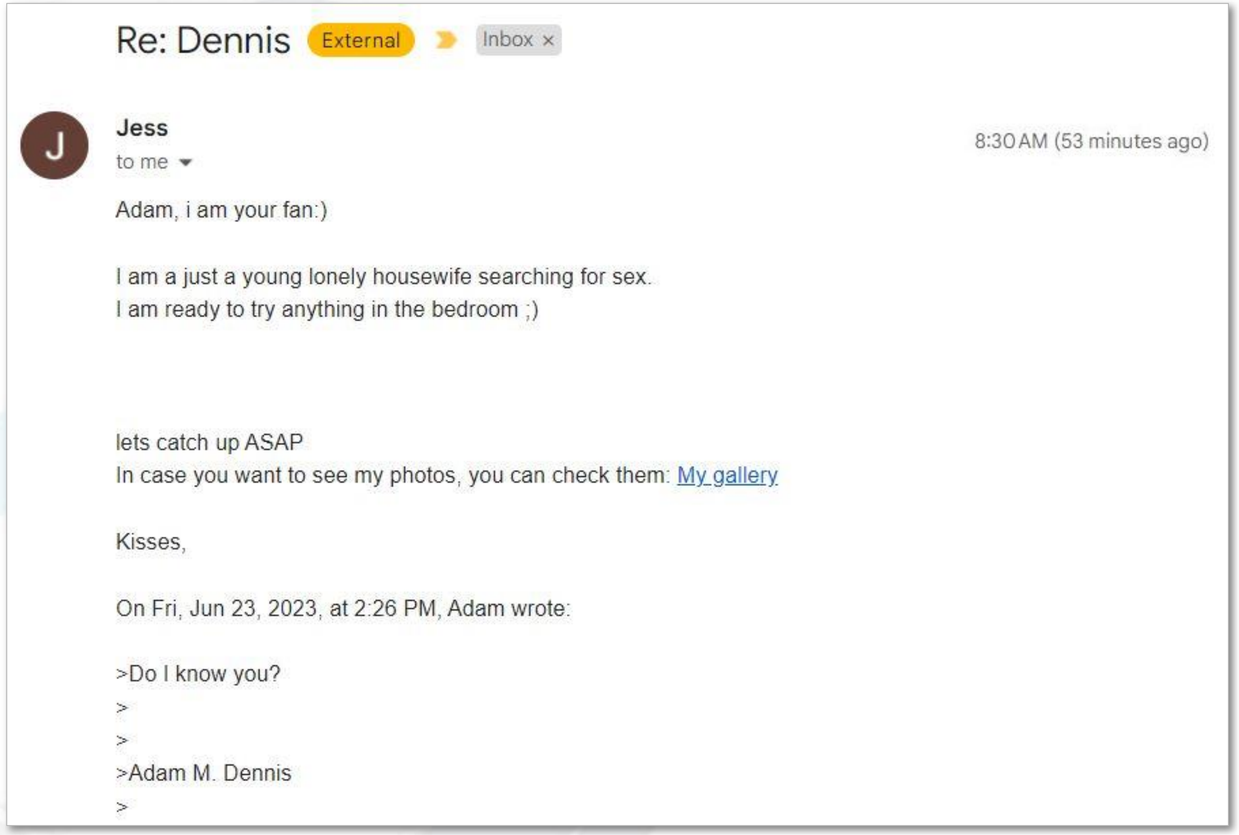
1. Visit suntrust.com
2. Sign on to Online Banking with your user ID and password
3. Select your account

We appreciate your business and are committed to helping you reach your financial goals. call us at 800-SUNTRUST (786-8789), or stop by your local branch to learn more about our helpful products and services.

Thank you for banking with SunTrust.

Sincerely,
SunTrust Customer Care

https://us.norton.com/blog/online-scams/phishing-email-examples



Re: Dennis External Inbox ×

J

Jess
to me

8:30 AM (53 minutes ago)

Adam, i am your fan:)

I am a just a young lonely housewife searching for sex.
I am ready to try anything in the bedroom ;)

lets catch up ASAP
In case you want to see my photos, you can check them: My gallery

Kisses,

On Fri, Jun 23, 2023, at 2:26 PM, Adam wrote:

>Do I know you?
>
>
>Adam M. Dennis
>


Cyber security advice:
If a girl texts you first,
block him.

Email Phishing... Examples

Typical Examples?

Loan fee fraud and scams

Angler Phishing (Hint: Think customer service)

Social Engineering

Invoice fraud

Whaling

Job scams & employment fraud

Cloning of reputable companies

Clone Phishing

Catfishing

Spear Phishing

Final request text scams

Vishing

Email Phishing

Water Hole Phishing

Investment scams

Bank Phishing Emails & SMSs

Pharming

Pop-up Phishing

* CGSO and Norton

Email Phishing...

What to Do If You are Caught in a Phishing Attack

1. **Change affected passwords** immediately (including other accounts where the password may have been used (bad idea!)... not using the computer that was compromised.

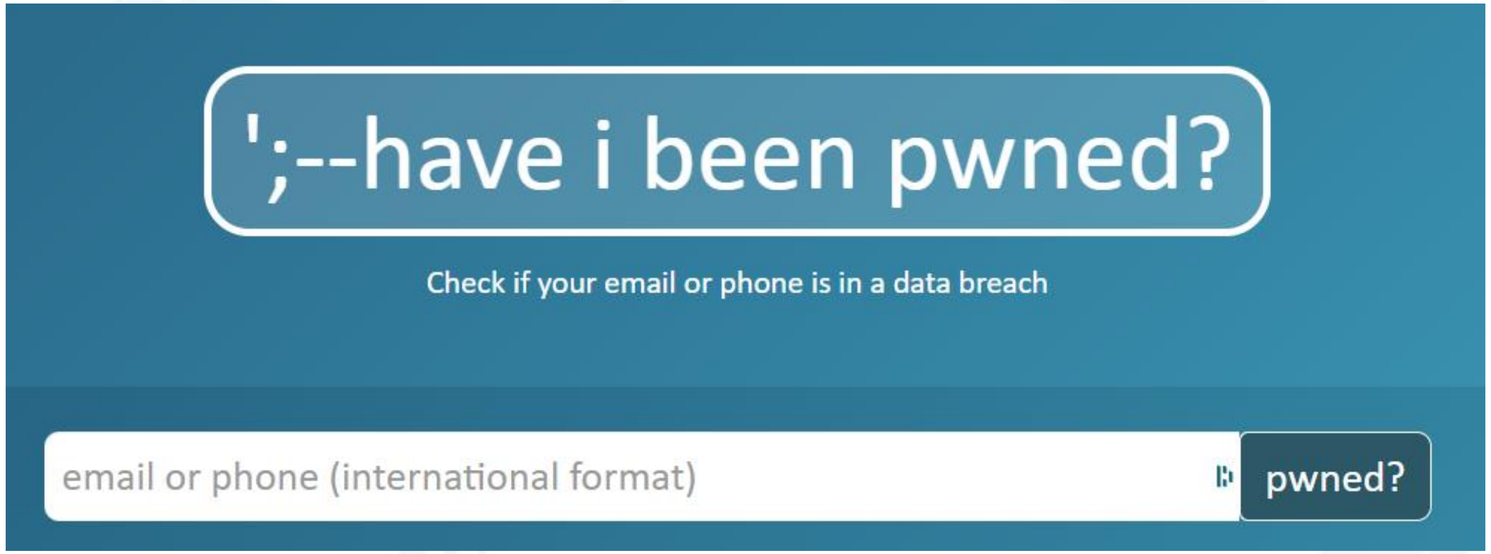
2. **Contact the fraud department of the breached account** – If the phishing attack compromised a bank or other critical account (like credit cards), contact their fraud department immediately.

3. **Notify appropriate people in your company** – Follow your company's incident response plan to ensure the appropriate personnel are aware of the incident starting with IT.

4. **Notify affected parties** – If personal data of others (e.g., customers, suppliers) was compromised, be sure to notify them to enable to protect themselves as well.

An Informative Break…

A Quick Resource to Check If You've Been Compromised…



haveibeenpwned.com

Email Phishing...

Ways to Protect Yourself Against Phishing Attacks

1. **Use AV software** – Up-to-date anti-virus software may help prevent the malware from installing.
2. **Utilize email filters** – Many email services have configurable filters which can help prevent many phishing messages from ever reaching users' mailboxes.
3. **Configure email security tech** – email services can also implement email authentication tech that can verify and reject messages that are spoofed.
4. **Activate anti-phishing functionality** for email clients and web browsers that have anti-phishing capabilities.
5. **Implement multi-factor authentication (MFA)** – If MFA is enabled, an attacker may still not be able to access your account even if you are tricked into providing your password.

RaaS tools [operate as] a subscription service like Netflix or Hulu, but instead of having access to movies and TV shows, you get software that can decode and encrypt most vulnerable systems effortlessly. This provides a steady stream of income for the RaaS owner and more successful ransomware attacks for the hacker.

- Norton (2023)

Ransomware Attacks...

Ransomware Attacks - What, Why, & Outcomes

1. Type of **software with malicious intent** and a threat to harm your data
2. Author or distributor **requires a ransom to undo** the damage
3. **Ransom payments don't always work**.
4. Ransom often needs to be **paid in cryptocurrency**.

Remedies - Prevention -

1. **Update and patch** your computer.
2. **Use caution** with links and when entering website addresses.
3. Open email attachments with **caution**.
4. **Keep personal information safe.**
5. **Verify email senders.**
6. **Use a VPN & avoid public Wi-FI**.
7. Use and maintain **preventative software programs**.
8. Regularly **back-up data** on a cycle.

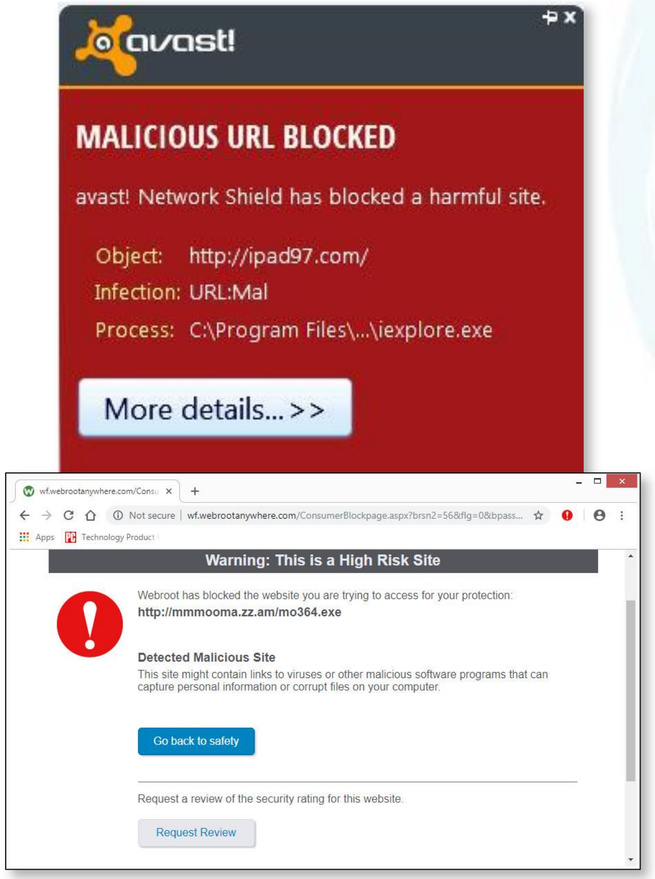
Remedies - Responses -

1. **Individuals:** Immediately notify local law enforcement and seek assistance in cleaning your device.
2. **Organizations:** Immediately report incidents to your IT department and local law enforcement, if necessary.
3. **All users:** Change all system passwords once the ransomware has been removed! (See Choosing and Protecting and Passwords and Supplementing Passwords.)

Quiz Time!

FTC Phishing Quiz

Malicious Websites & SMishing



Malicious Websites

1. **What are Malicious Websites?**
   Sites that attempt to install malware (aka software that will disrupt computer operation, gather your personal information, or gain total access to your machine) onto your device. This usually requires some action by you, but in some cases a website might attempt a “drive-by download” of installing software without asking first.

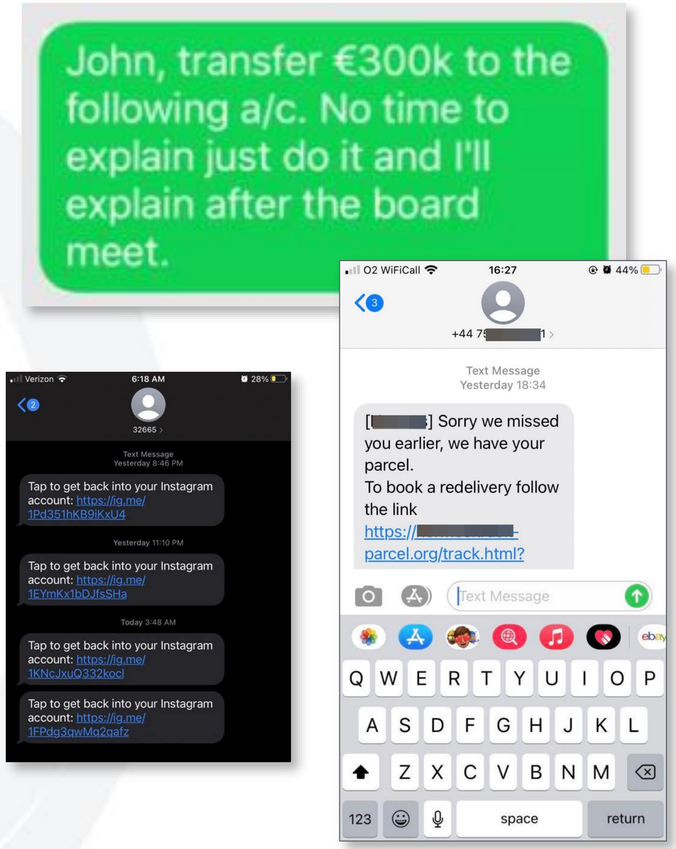
2. **How to Handle…**
   a. Double-check the URL and security status.
   b. Use antivirus software that scans for, and provides warnings about, malicious sites.

Malicious Websites & SMishing…

SMishing

1. **What is SMishing?**
   Attacks instigated through Instagram, LinkedIn, Facebook, Twitter, TikTok and other social media platforms.

2. **How to Respond…**
   a. If you receive a DM from a suspicious account, or just someone you don't know, delete and block it. DO NOT engage!
   b. If you receive a DM for a person you know, confirm that they sent it to you before you act… and make sure that they didn't just forward it through to you and a bunch of other people!



Social Engineering

What is Social Engineering?

+ Trickery
+ Charming Authority
+ Manipulation
+ Impersonation
+ Deception
+ Access to information

The 4 Steps

1. **Preparation:** Social engineer gathers info about their victims, including where they can access them, such as on social media, email, text message, etc.
2. **Infiltration:** Social engineer approaches their victims, usually impersonating a trustworthy source and using the information gathered about the victim to validate themselves.
3. **Exploitation**: Social engineer uses persuasion to request info from their victim, such as account logins, payment methods, contact information, etc., that they can use to commit their cyberattack. Attack often starts with innocuous info requests.
4. **Disengagement**: Social engineer stops communication with their victim, commits their attack, and swiftly departs.

Social Engineering...

Social Engineering Explained

Also known as human hacking, social engineering is the manipulation of someone to divulge confidential information that can be used for fraudulent purposes.

1

The social engineer gathers information about their victims.

2

The social engineer poses as a legitimate person and builds trust with their victims.

3

The social engineer gathers information about their victims.

4

The social engineer poses as a legitimate person and builds trust with their victims.


I'm sorry. My-
REAL FUTURE

According to an annual report on global cyber security, there were a total of 304 million ransomware attacks worldwide in 2020. This was a 62% increase from a year prior, and the second highest figure since 2016.

- Statista.com

Social Engineering...

Social Engineering Examples

Scareware

Email hacking

Access tailgating

Phishing

DNS spoofing

Baiting

Physical breaches

Pretexting

Watering hole attacks

Quid pro quo

Social Engineering...

Rules for Safe Online Communications

1. **Don’t click links you don’t request**.
2. **Don’t overshare** personal information online (Turn off location on your phone!).
3. **Be cautious** of online-only friendships.
4. **Remember the signs** of social engineering.
5. If it’s **too good to be true**...
6. Do not use Social Media if you can.

Secure Accounts and Networks

1. Use **two-factor authentication**.
2. Only use **strong, unique passwords**.
3. Consider a **password manager** to keep track of your passwords.
4. Enable **aggressive spam filters**.
5. **No strangers on your Wi-Fi** network and **updated router pwds**.
6. **Use a VPN**.
7. **Monitor** your account activity closely.

Safeguarding Your Devices

1. Don’t leave devices **unattended**.
2. Use **cybersecurity** software.
3. Keep your **software up to date**.

HOW PASSWORD LENGTH WINS THE INTERNET

Passwords 102

Password Guidelines…

Prudent Password Guidelines

The key to creating and storing strong passwords…

1. **Length:** Minimum of 15-64 characters. Use a password generator (and vault), if possible. This is the single most important factor.
2. **Complexity:** Mix it up with upper case/lower case, spaces, characters and numbers!
3. **Unique:** DO NOT REUSE PASSWORDS. Need I say more? For “fun”, check “**Have I Been Pwned?**” for your email and password.
4. **Uncommon:** Don’t include well known phrases, quotes, or lyrics.
5. **Don’t Share:** Yes, I need to say this: Don’t share your passwords.
6. **Use a Password Manager/Vault:** But make sure that your passphrase is very long to protect the master login. Do the same for your email account since that is usually the achilles heel for most secure systems. **Recycle every 30 days**.

SECURITY GRAB BAG

Physical Security Scenarios

Real World Scenarios

At Work

A senior partner at a consulting firm drives to work each day and uses her access badge to enter her company's floor. No badge is necessary in the office, but one is needed to use the stairs to access other offices. The partner brings her laptop home each night, but locks it in a desk drawer when she is not going home directly.

One evening she rushes out the door to meet a client for dinner. Before leaving, she quickly clears her desk of papers, stuffs some in the desk, locks up her laptop, but does not check the floor around her desk. Moreover, she forgets some papers in the printer.

At Home

A VP spends 80% of his week working from home, and the other 20% traveling, or at a local diner. He is careful and uses a secure wireless network or the company's MiFi along with a VPN. In public, he also employs a screen protector on his laptop so that his screen cannot be easily viewed by others. When traveling, he turns off his laptop and leaves it in his hotel room or, when driving, he stores his laptop in the trunk of his rental car.

One day, after working late at home, the VP left his laptop on when he went for dinner. His son then used his laptop to search for a video game on a gamers' forum and clicked an ad link on the website.

Physical Security Consequences

Real World Consequences

At Work

THE GOOD

1. **Locking up the laptop**…
2. **Using her badge**… and
3. **Clearing the papers** are all good security practices.

THE BAD

1. Leaving **documents at the printer** is one of the most vulnerable spots in an office setting. If a doc contains sensitive client information, this is a high-risk security event if the doc contains NPI or proprietary info that others in and out of the company should not see.
2. **Not checking around the desk** can miss papers that might contain critical information like written down NPI.

At Home

THE GOOD

1. The vice president is following a security best practice by **using the company's MiFi** network, which is good.
2. By only **using secure networks,** he does not make his laptop vulnerable to hackers.
3. Finally, **using a privacy filter screen** is a good idea to keep sensitive information from being widely visible in a public place.

THE BAD

1. **Leaving the laptop unlocked** is a bad idea, even in his own home.
2. While his son did not expose his laptop to a virus, any **unrestricted browsing** that leads to sites unrelated to business could potentially lead to a security threat for the entire network.

Physical Security…

Rules of the Road

1. **Don’t** leave important papers on your desk overnight.
2. **Never** use a stray thumb drive and insert it into your computer. Such devices can contain malware that could infect your computer.
3. **Check** the printer before you leave the office to confirm that you haven’t left sensitive documents in the printer tray.
4. **Always** lock your computer when you step away from your desk – even if you are only gone a few minutes (and at home!).
5. **Never** use an open Wifi network, check that AP isolation on your Wifi router is enabled, and don’t charge your phone on a public USB outlet unless your phone is off.
6. Get a full **threat assessment** of your potential vulnerabilities.

A Little Extra

Best Practices Regarding Passwords and PPI

1. **Don’t** ever **share passwords**, even with a close friend.
2. **Don’t** ever **send private information** via email or any other insecure communication medium.
3. **Always segment access to PPI** whether it is staff, or a third party.
4. **Store PPI for only as long as necessary**. Purge unused records automatically.

Quiz Time!

Physical Security Quiz

Time to Wrap Up!

What Did We Learn? Let's talk.

A Quick Review…

- Why Hackers Hack
- Cybersecurity Objectives
- Phishing and Ransomware Attacks
- **How to Protect Against Phishing Attacks**
- How to Protect Against Ransomware Attacks
- How to Protect Yourself Against Malicious Websites
- What is SMishing?
- Explain Social Engineering
- Examples of Social Engineering
- **How Not to Get Tricked** … Zero Trust!
- Rules of Safe Online Communications
- Hacking Examples
- Ways to Prevent Hacking
- Types of Password Attacks
- Strong Password Guidelines
- **Which is Better?** Password Length or Complexity?
- Why is Physical Security Important?
- Password and PPI Best Practices

Tool Tips and Simple Security Policies

Useful Tools for Secure Surfing (Only download from official websites!)

1. Use **antivirus software** such as Windows Security (comes with Windows), Norton, or Kaspersky.
2. Use a **VPN** such as NordVPN or ExpressVPN.
3. Use a **password manager/vault** such as NordPass or LastPass (to also create random long-form passwords of 15-20 characters).
4. Use a **data breach scanner** such as that provided by NordPass or HaveIBeenPwned? to periodically scan for breaches involving your email account(s).
5. Use a **malicious website extension** such as Norton Safe Web, TotalAV Safesite, and/or https everywhere.

Simple Policies to Protect You and Your Business

1. Enforce an **automatic password change** every 30 or 60 days. It's a pain, but it's worth it.
2. Engage **automatic updates** for all your devices and software
3. Engage multi-factor authentication (**MFA**) on critical accounts such as email (ideally using an authenticator or your phone).
4. **Backup critical systems** regularly keeping a 2 week and a 30 day copy coupled with incremental backups daily.
5. **Store your critical content** securely on a Cloud server.
6. Make sure you only visit websites that use **https**.
7. Use **safe words** for critical relationships… business and personal.

A Call for Resiliency

The Building Blocks of Resiliency

The concept of "**Cyber Resiliency**" has to do with the questions of how well you are prepared to counter disruptions from cyber-attacks, and how quickly you can recover from them. Below are three rules recommended by the *World Economic Forum* to consider in your resiliency planning:

1. **Cyber Resiliency Planning Must be Directed from Top Executives:**
   a. Leaders must come to better understand the **threat landscape**; and
   b. Executives should nominate **one person to regularly report** on risks and mitigation strategies such as **planned vulnerability assessments, pentesting, and simulated phishing attacks or backup and recovery policies**.

2. **Cyber Resilience Must be a Core Business Goal:**
   a. Leaders must **invest in defensive, preventative, and reactive initiatives** alongside recovery capabilities; and
   b. Build cyber literacy in their staff emphasizing a "zero trust" and "always verify" models.

3. **A Commitment to Resilience Enables Positive Business Outcomes:**
   a. Businesses must **align their planning with risk tolerance**; and
   b. Understand the types of attacks that would compromise critical business activities.

RESOURCES & TOOLS

Resources and Tools

Resources

1. **NIST.gov:** Resource provided by the US Department of Commerce's National Institute of Standards and Technology. To search for information, select the search function in the top right of the navigation.
2. **CISO.org:** US Cybersecurity & Infrastructure Security Agency. Great for researching and reporting incidents.
3. **Norton.com:** Great resource to search for information about cybersecurity awareness content.
4. **TrendMicro.com:** Another resource that can be used to search for cybersecurity awareness content.
5. **Kasapersky.com:** Their Resource Center is a great place to further your education.
6. **The People Hacker - Confessions of a Burglar for Hire, Jenny Radcliffe:** Excellent book on social engineering.
7. **Forvis:** The full text of the real world scenarios discussed for physical security. Good source of other info.
8. **World Economic Forum:** 3 principles to help build a cyber resilient organization.
9. **Reporting: CID and ONDCP:** For local Antiguan reporting. Note that in cases of losses of money, the sooner you contact the ONDCP, the better especially if the money has been routed through a foreign bank.

Resources and Tools...

Tools

1. **Have I Been Pwned?:** Excellent tool that you can use to research if your phone or email has been included in a data breach.
2. **Password Manager Options:** The list provided here covers a range of options identified by PCMag. Each has its adherents and detractors. Your final decision should include feedback from your IT Department (which might require a specific option) and/or consideration of the security solution you are using on your computers since the solution might include its own password manager.
3. **Top 10 VPNS:** Again, the list is offered by PCMag and you should apply the same decision-making logic as recommended above for the password manager.
4. **Cybersecurity Awareness Quizzes:** Whether for your staff, or for self-training, these quizzes are good options for testing your knowledge, or that of your staff.

HOW TO REACH US

+1 268.764.8362

antiguarecon.com

adam@antiguarecon.com