Bar Harbor Business Online

Guide to Online Threats, Controls and Best Practices

BAR HARBOR
BANK & TRUST

Personal Banking — Business Banking — Wealth Management

"The American government, American businesses, and Americans themselves are attacked over the internet on a daily basis,"
Chairman Steve Chabot (R-OH) said in his opening statement.

"Sometimes they know, sometimes they don't. These attacks come from criminal syndicates, 'hacktivists,' and foreign nations. They're after intellectual property, bank accounts, Social Security numbers, and anything else that can be used for financial gain or a competitive edge.
But the majority of cyberattacks happen at small businesses.

In fact, 71 percent of cyberattacks occur at businesses with fewer than 100 employees."

https://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=398099

Table of Contents

Background

Enrolling your business in Bar Harbor Business Online services can offer a convenient and operationally effective way for you to conduct complex banking processes directly from your business; however, there are inherent dangers and risks associated with internet banking. It is important to note that businesses are not protected by the same regulatory rights that consumers are. In 1978, Congress passed the Electronic Fund Transfer Act (Reg-E) to protect individual consumers engaging in electronic fund transfers, those same protections are not extended to businesses conducting electronic fund transfers. If fraudulent, unauthorized, or otherwise mistaken electronic fund transactions occur, your business may be fully liable.

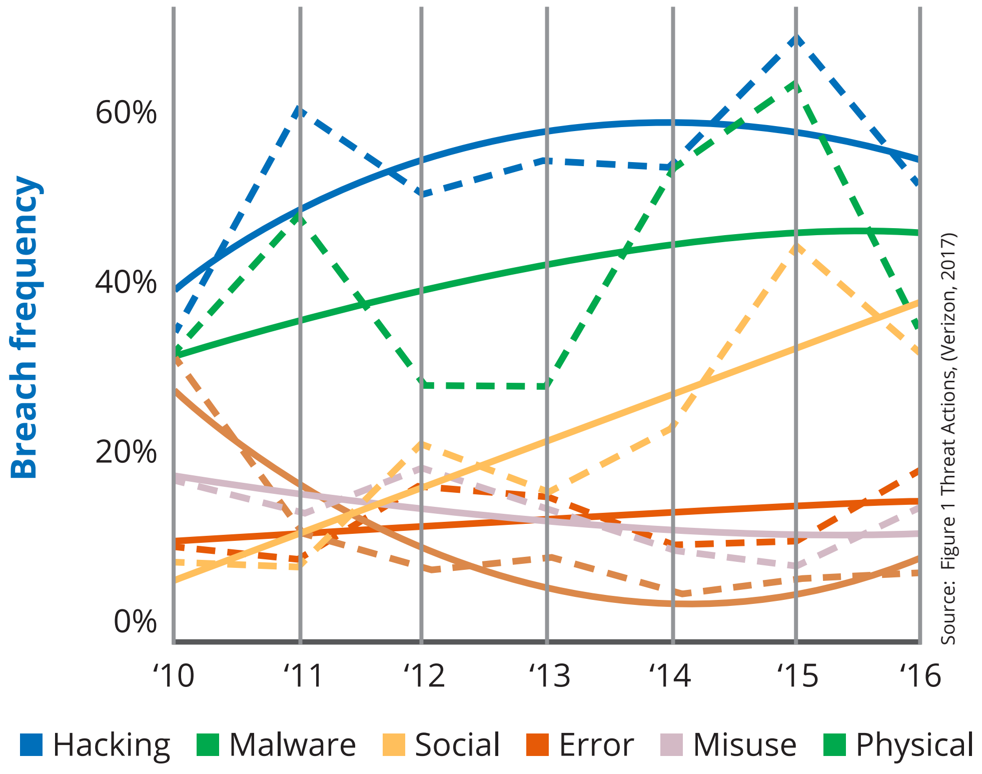
Please take the time to fully understand the risks associated with online banking, know the threats, and understand your vulnerabilities.

If you are considering or have already enrolled in Bar Harbor Business Online services, we recommend you take the time to read this document. The document is divided into 5 security topics:

1. External threats targeting your business through the attempted exploitation of your employees
2. Internal threats that may already be lurking within your infrastructure
3. Responsibilities you must acknowledge to adequately manage risk
4. Controls the Bank has implemented to help you manage internet banking risks
5. Strongly recommended best practices for securing your business

Section 1: External Threats

Cyber threats designed to take over end-user e-commerce transactions and banking sessions continue to increase year over year. Not only has the volume of attacks continued to rise but the diversity of those attacks continue to expand into new avenues. External threats most commonly present themselves via email or through web browsing. Hacking, malware, and social engineering (i.e., phishing) are the most prominent threat actions an external attacker will use to compromise your banking credentials/session. Sophisticated adversaries will blend threats to craft an attack and persist as long as their resources will allow.



Source: Figure 1 Threat Actions, (Verizon, 2017)

Since 2010, **hacking** has been the most prominent threat action in data breaches analyzed by Verizon (Verizon, 2017). Your business may or may not have a point of presence (i.e., website) that is susceptible to external hacking. The same cannot be said for your employees. Attackers may hack your employees indirectly via social networking sites or by learning their password through data dumps from websites that have been breached.

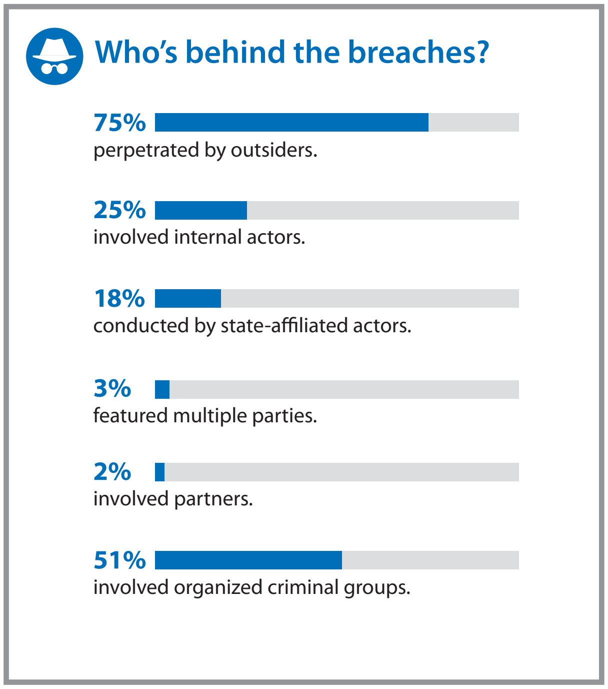
Malware targets all organizations regardless of size or complexity. **Malware is most frequently introduced to a business via email;** however, malware also commonly lurks on **compromised** websites. Malware can self-propagate across file shares or by sending copies of itself to the contacts of a user using an infected computer. The 2017 WannaCry Ransomware outbreak was fueled by the ability of the malware to propagate across file shares. This document will describe cybersecurity best practices that can help prevent your organization from being adversely affected by malware. Most malware though, requires human intervention to unleash the damage.

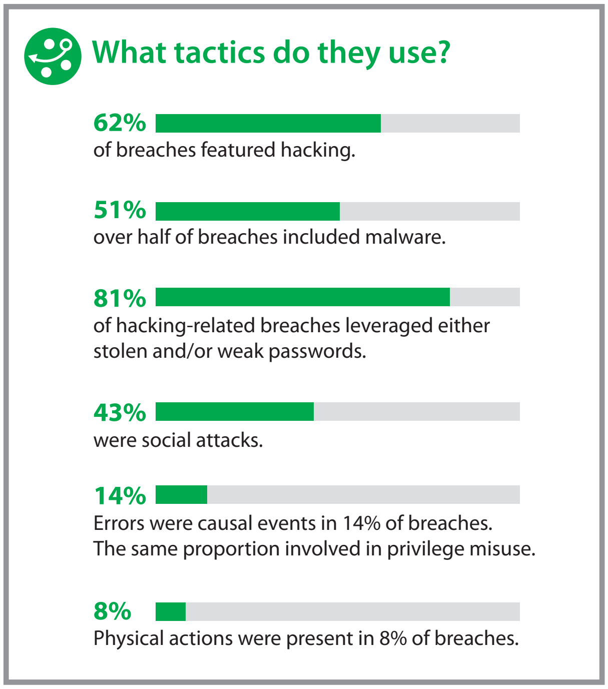
WannaCrypt used EternalBlue, an exploit for a previously fixed SMBv1 vulnerability, to propagate itself across networks rapidly, affecting a large number of computers in a short time. (Microsoft released Security Bulletin MS17-010 in March of 2017 to address the vulnerability.)

Source: Microsoft 2017

Keeping your operating systems and software up to date is critical! It can save your business time and money.

Social engineering is the catalyst malware needs to infect your business. Social engineering attacks are growing steadily and are used in 43% of attacks. Criminals may cast a wide net, sending thousands of email messages, hoping to entice any trusting human using a vulnerable computer into opening a malicious attachment or following a link to a malicious website. Attackers who are focused on targeting a specific industry, organization, or employee can "hack" the target entity via public internet data stores and tailor their subsequent spear phishing attack to achieve a greater likelihood of successfully exploiting their target.





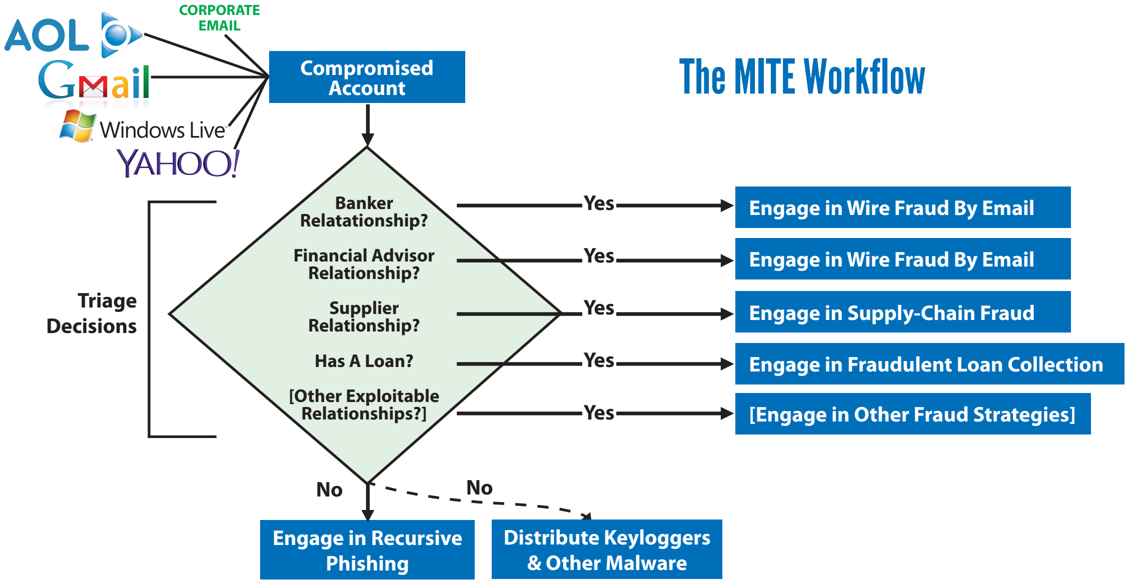
Source: 2017 Breach Data, Verizon 2017 Executive Summary

Employees are a key defense against all threat vectors. Employee security awareness programs should emphasize the email threat vector. Email is the most common method to deliver malware, the email recipient ultimately must decide whether to click a link or open an attachment. It is important to understand your employees are either your last line of defense or your weakest link. **"Your employees and your business partners can be potential threat actors or targeted victims. It is important to not lose sight of the role humans play in data breaches (Verizon Enterprise, 2016)."**

This document provides best practice guidance to mitigate the risks most prevalent in the threat landscape facing your business today. We have identified some of the most prevalent threat vectors below:

Email Threats

Email messages originating from external attackers but purporting to be a vendor you routinely do business with, can be armed with a malicious attachment or a link to a malicious website. Too often, these messages make it past defenses and land in the inbox of any one of your employees.



The MITE Workflow
AOL
Gmail
Windows Live
YAHOO!
CORPORATE EMAIL
Compromised Account
Triage Decisions
Banker Relatationship?
Financial Advisor Relationship?
Supplier Relationship?
Has A Loan?
[Other Exploitable Relationships?]
Yes
Yes
Yes
Yes
Yes
Engage in Wire Fraud By Email
Engage in Wire Fraud By Email
Engage in Supply-Chain Fraud
Engage in Fraudulent Loan Collection
[Engage in Other Fraud Strategies]
No
No
Engage in Recursive Phishing
Distribute Keyloggers & Other Malware

Business Email Compromise (BEC) or man-in-the-email (MITE) scams are adaptive and surprisingly complex.

Source: Krebs

Phishing

Phishing email campaigns sweep across the internet at a large scale attempting to entice one in many users to take the bait. Verizon reports that 7.3% of users will fall victim to phishing campaigns. A phishing email may entice recipients to click a link to access data of interest on what appears to be a legitimate website, e.g., Microsoft OneDrive, Google Drive, Dropbox, or your Bank; but the website is actually a malicious imposter website that prompts unsuspecting victims for some form of personnel information (log-on credentials, personal nonpublic information). A common weak security practice is for end users to reuse the same password on multiple sites, the reuse of passwords offers the attackers hope of collecting more versatile credentials that can even allow direct access to corporate accounts. Phishing emails may also contain malicious attachments that attempt to download and execute malware in the context of the user. In this scenario, the attacker attempts to gain a foothold on the user's computer which may be on your business network.

You can help protect your business from risks associated with Phishing threats by implementing the following BEST PRACTICES:

- Provide your employees with security awareness training so they can spot phishing attempts.
- Do not permit email access from privileged administrator user accounts.
- Do not reuse passwords across multiple accounts/websites.
- Enable multifactor authentication wherever possible.

> **“Spear-phishing emails emerged as by far the most widely used infection vector, employed by 71 percent of groups.”**
>
> Source: Symantec, 2018

Business Email Compromise

Business Email Compromise (BEC) is a targeted phishing attack/exploit in which the attacker gains access to a corporate email account and spoofs the company owner and/or company executive to defraud the company or its employees, customers, or partners of money. The personalization combined with some element of urgency makes this a frequently lethal technique. This especially threatening attack is specifically targeted and does not involve malware, making it very difficult to detect. Trusted employees unknowingly execute the nefarious task thinking you (the owner of your business or some other high-ranking executive within the organization) asked them to. The threat’s success rate stems from the fact that when we receive email from a contact we naturally assume that it was sent by them. The offending email directs the recipient to perform some action and believing it was sent by company leaders, they carry out the instructions. Unlike an anonymously written note, most people just don’t question the sender of an email. Those most likely to be BEC targets are those who work closely with executives including your accounting and human resources teams. BEC scams hit 7,710 organizations every month (Symantec, 2018).

You can help protect your business from risks associated with BEC threats by implementing the following BEST PRACTICES:

- Do not initiate important transactions via email request.
- Encourage employees to be suspicious of any email requests which convey a sense of urgency or secrecy.
- Provide security awareness training for your employees.

Top subject lines in BEC scam emails

Analysis of the BEC emails shows that the most frequently occurring words included, “payment,” “urgent,” “request,” and “attention.”

Rank	Subject	Percent
1	Payment	13.8
2	Urgent	9.1
3	Request	6.7
4	Attention	6.1
5	Important	4.8
6	Confidential	2.0
7	Immediate Response	1.9
8	Transfer	1.8
9	Important Update	1.7
10	Attn	1.5

Source: Symantec, 2018

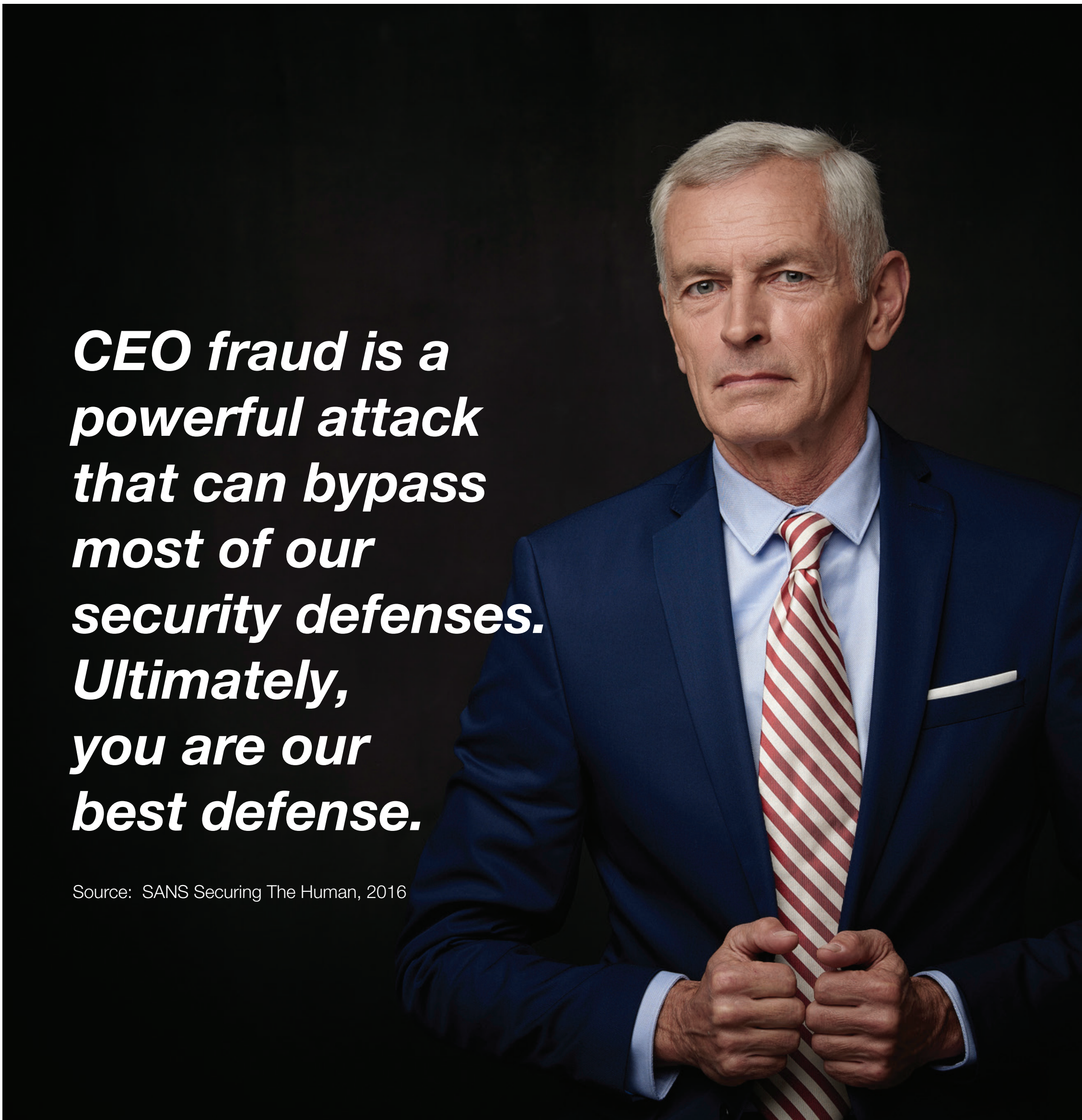
A single web page may consist of hundreds of individual elements. Your computer makes hundreds of ***web requests****, one for each individual element, to load a single web page. Any one of these elements could be malicious. These subtle threats are referred to as* ***drive-by downloads****.*

Web Threats

A compromised website can deliver malware to your computer. One in 13 web requests lead to malware (Symantec, 2018). Malware perpetrators easily discover thousands of vulnerable websites via automated scanning routines and stage them with malware. These infected websites await unsuspecting visitors and automatically drop malware via a drive-by download. In a more targeted scenario known as a watering hole attack, the attacker intentionally compromises a website that your business frequents.

You can protect your business from risks associated with Web Threats by following these BEST PRACTICES:

- Train your employees to heed web browser warnings.
- Implement a web filter or web proxy to block internal requests to high-risk websites.
- Install a reputable antivirus program and be sure it is up to date.
- Ensure that your computer's operating system and programs have automatic updates enabled.



CEO fraud is a powerful attack that can bypass most of our security defenses. Ultimately, you are our best defense.

Source: SANS Securing The Human, 2016

Specific Types of Attacks

Account Takeover

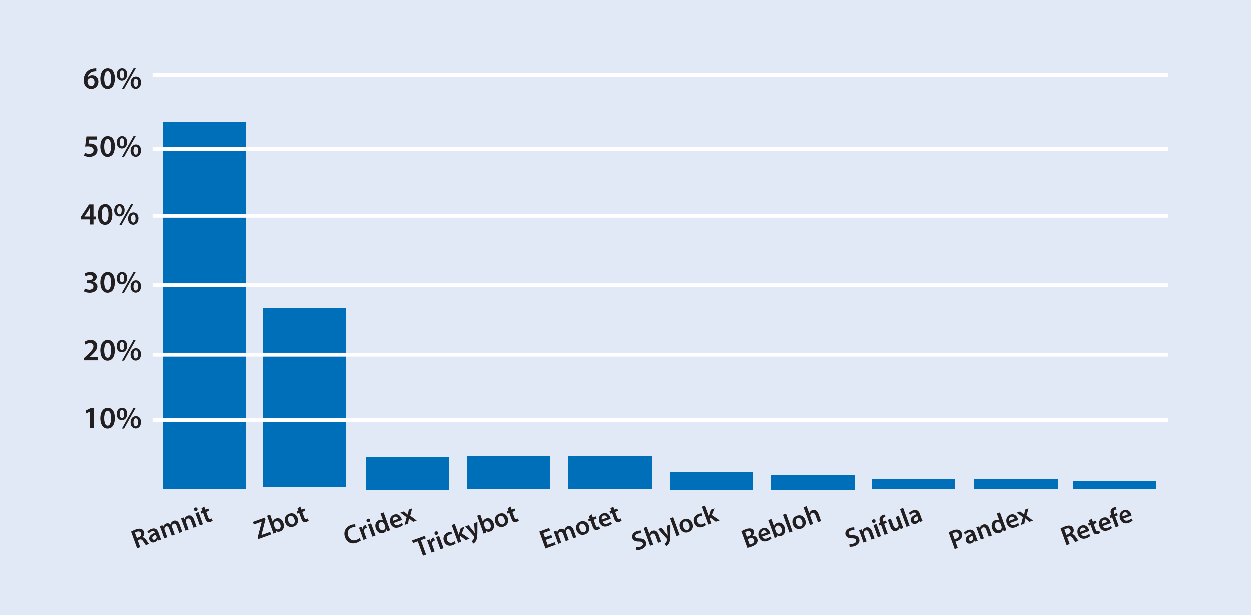
Account Takeover (ATO) is a type of fraud where threat actors gain control of online accounts and then make unauthorized transactions from the compromised account. ATO is the most common and dangerous scam for small businesses (Federal Deposit Insurance Corporation, Winter 2011/2012). Account takeover can stem from malware delivered via email or a compromised website. The malware monitors and records websites and keystrokes on infected computers and may spread to other victims discovered in the user's email contacts. Your online banking log-in credentials are stolen and sent to the attacker. The attacker has control of the victim's computer, has access to your business accounts, and control of your money. How long will it take for your company to detect an ATO?

Reduce the risk of ATO by implementing the following BEST PRACTICES:

- Avoid online banking transactions on computers used to check email or browse the web.
- Implement segregation of duties/dual-control approvals for payment channels.
- Utilize strong multifactor authentication.
- Use value-added services such as Positive Pay and ACH Debit Filters.
- Monitor your accounts daily to detect unauthorized transactions.

Top 10 Financial Trojans 2017

Ramnit and Zbot dominated, but Emotet the fifth most detected, made a big impact towards the end of the year.



Source: Symantec, 2018

"Dridex (Trojan.Cridex), which is third in our top 10 list of financial Trojans for 2017, now checks the software installed on the devices it has infected. If it detects accounting software, it will enable remote access and attempt to carry out larger fraud, rather than just stealing online banking credentials."

Source: Symantec, 2018

UPDATE:

Emotet was noted by Symantec in their 2018 Internet Security Threat Report as having had a breakthrough late in 2017. Emotet continues to be on the rise and has evolved from targeting banks to a modular delivery platform targeting both the public and private sectors.

Ransomware

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to the data unless a ransom is paid to the threat actors. Ransomware is a profitable business. The sole potentially positive aspect about some "trustworthy" Ransomware is that your data may not become exposed and you can pay your way out of it. The risk of Ransomware was initially driven by opportunistic infections of home users but has taken a turn toward being used in targeted attacks on organizations (Verizon).

You can help protect your business from Ransomware risk by following this BEST PRACTICE:

- Back up your data and store it somewhere safe.

Mobile Malware

Mobile malware is malicious software that is specifically built to attack smart phones and tablets. Security firm Symantec reports a 54% increase in the number of identified mobile malware variants in 2017. That is 9,365 new malware variants. Many mobile apps that are not outwardly malicious have a tendency to leak potentially sensitive information, such as the device phone number or location (Symantec, 2018).

Mobile devices started as personal data assistants and still are just that, personal. The trouble with personal devices is they are **(un)**managed by each individual. Mobile device operating systems are automatically updated by providers — until they are not! Mobile device hardware needs to be replaced every few years to keep current with mobile operating system releases which remediate vulnerabilities. Older mobile operating system releases are not maintained indefinitely. The most vulnerable component of mobile devices is the owner. Individuals need to **configure screen locks** and **encrypt** their devices. It is also a good idea to **enable location tracking** for when it does get lost. And enable **automated backups** for when it cannot be found. The screen lock and encryption will keep the data protected from whoever does find it.

You can help protect your business against Mobile Malware by following these BEST PRACTICES:

- Configure device auto-lock and require a password or biometric method to unlock.
- Enable device encryption.
- Enable automatic data backups.
- Enable location tracking.
- Organizations should consider mobile device management to provide remote wipeability.

Other External Threats

Be very cautious about exposing internal production systems/services directly to the internet. Many businesses will simply have no need to permit internal systems/services to be directly exposed to the internet. If you do not know if your business has internet-accessible service(s), then you need to check with your IT/Security staff or service providers. Securing corporate systems requires careful consideration and is beyond the scope of this document.

Point-of-Sale (POS) Attacks

Merchants who accept credit/debit card payments are subject to Payment Card Industry (PCI) compliance requirements mandated by major payment card brands. Many merchants will outsource their card processing to a third-party vendor to reduce both their risk exposure and the burden of PCI compliance; however, merchants will still assume some risk and burden if a breach occurs. It is the responsibility of each merchant to know their PCI merchant level and their associated PCI-compliance responsibilities.

Verizon described the attacks circa 2013 on internet-facing POS systems to be "smash-and-grab" operations (Verizon, 2017). Seemingly careless POS providers supplied their merchants with POS systems that had default credentials and were directly connected to the internet. Attackers had automated systems to discover and exploit these systems to steal card data. Current POS fraud trends are for attackers to steal the vendor credentials at some link in the service delivery chain and then exploit the merchant's POS system. The take-away is to understand the risks around accepting card payments and do your homework when selecting a POS vendor or merchant services provider.

The following BEST PRACTICES apply to merchants who accept cards:

- Select a reputable POS provider and ensure they take security seriously. Ask how their services and systems comply with PCI security standards.
- Isolate POS equipment on a dedicated network and restrict network access.
- Have a PCI Security Standards Council Approved Scanning Vendor (ASV) conduct regular scans of your POS environment.

Section 2: Internal Threats

In Section 1 we described external attack vectors: Hacking, Malware, and Social Engineering. Section 2 of this document is dedicated to common internal threats: Insecure Systems, Errors, Misuse, and Physical Threat Actions. These threats do not get the same publicity/attention as external threats, but they generally hit closer to home and are a real threat to businesses of all sizes. The success of an external attack is often enabled by vulnerabilities that are already present inside of an organization's technology environment.

Unauthorized Devices

Unauthorized devices connecting to your network present unknown threats. A multitude of gizmos with embedded computers and network connectivity make up the **Internet of Things (IOT)**: smart TVs, surveillance cameras, automation devices, environmental and health monitors, etc. Software in IOT devices may never be updated and therefore have a higher probability of exposed vulnerabilities. The proliferation of internet-aware devices makes them a literal **honeypot**. IOT devices enable the tech-savvy insider threat you did not know you had to become a reality.

Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank.

"The attackers used that to get a foothold in the network. Then they found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."

Source: Williams-Grut, 2018

USB Devices

A brief word on **USB storage devices** (i.e., thumb drives, USB sticks, flash drives): be wary of them. They can circumvent security controls and given their mobility and small size can be introduced where they are not wanted and deliver malware or enable exfiltration of data.

You can help protect your business against USB storage devices by following these BEST PRACTICES:

- Keep an inventory of authorized computers and networked devices, disable unused network ports, and secure your wireless networks.
- Disable removable storage device auto run on company computers.
- Block the use of USB storage devices on company computers.

Unauthorized Software

Unauthorized software is an unnecessary vulnerability. Modern operating systems have tremendous security features natively built into them; however, the same cannot be said for the myriad of software packages, some of which practically install themselves. Using a computer while logged on with administrative privileges enables the installation of unnecessary software. If a computer has been around for a while, have a qualified IT technician examine it and remove old and unneeded software.

You can help protect your business against the threat of Unauthorized Software by following these BEST PRACTICES:

- Avoid using a privileged system administrator account for routine tasks, such as checking email or web browsing.
- Restrict software installation to your technical staff.

Insider Threats largely fall into two event types, those that are entirely unexpected and those that are bound to happen.

Malicious employees likely already have the access they need to steal your company's money or sensitive information and detection of unauthorized activity can be difficult. Bad employees are implicated in 15% of data breaches. A company really has a problem if privileged IT employees go rogue.

Errors made by well-intentioned employees account for another 14% of data breaches (Verizon, 2017). Misdelivery, publishing, configuration, and disposal errors are inherent threats to any company. A well-designed system of checks and balances can help discover errors before someone else does.

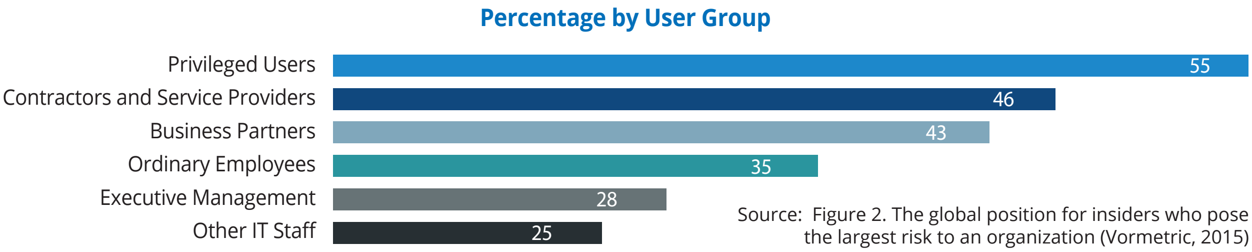
You can help protect your business against Insider Threats by following these BEST PRACTICES:

- Utilize dual controls and segregation of duties to help prevent mistakes and avoid a single employee having too much authority.
- Rotation of duties ensures that operations continue when employees are not available.
- Include background checks in new-hire screening processes.

Supply Chain, including technology and service providers, provides the materials and technology your business needs to function, but can also be used as a very effective attack vector. Forty-six percent of organizations indicate that contractors and service providers pose the biggest internal threat to corporate data (Vormetric, 2015). Do not assume Information Technology and Information Security is a package deal. Do not assume your service providers have robust security controls in place to protect your business. Implementation of proper security controls involves the commitment of both dedicated staff and the development of operational processes. Businesses that can't dedicate the resources to maintain a robust security environment should consider outsourcing as a feasible option.

You can help protect your business against Supply Chain risk by the following this BEST PRACTICE:

- Make security a requirement. Ask your service providers for a statement identifying how they protect your business (network, data, funds, etc.) and a statement of the vendor's internal security practices/controls.



Source: Figure 2. The global position for insiders who pose the largest risk to an organization (Vormetric, 2015)

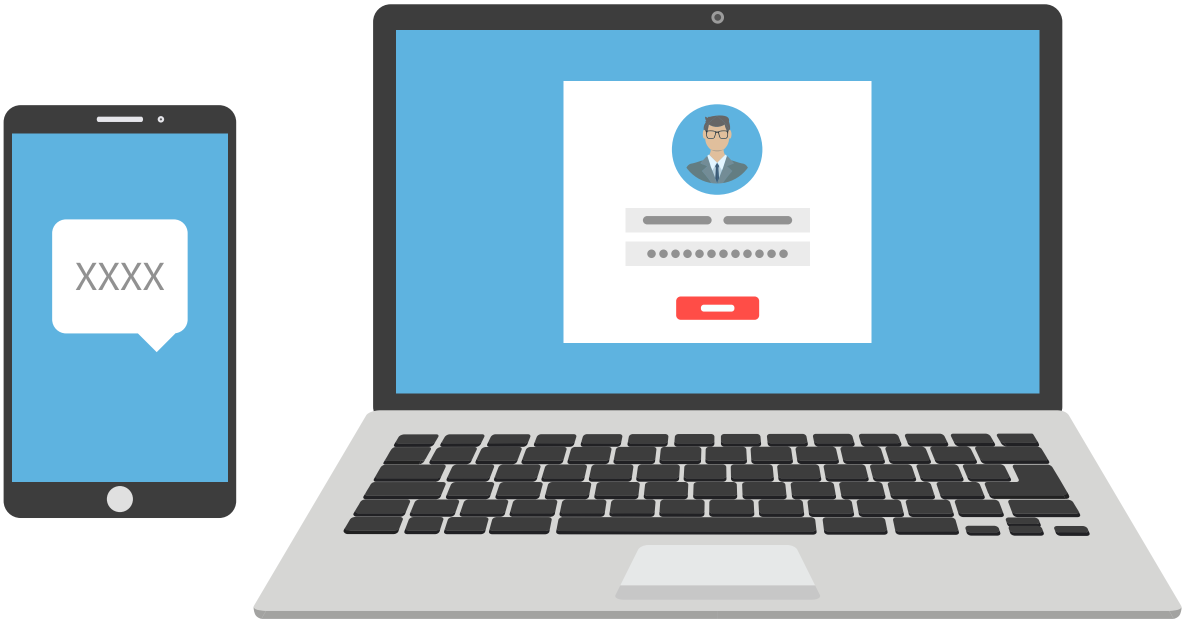
Other Internal Threats

Passwords

The strength/security of a password directly correlates to the password's complexity. Still, even the best passwords are easily lost to phishing incidents. Password guessing, password hash cracking, and password spraying can be combatted by automatic account lockouts, really long passwords (passphrases), and by not using the top 1,000 most commonly used passwords. The use of password managers does help, get one and use it, just not the sticky yellow paper kind.

You can help protect your business against Password threats by following this BEST PRACTICE:

- Enable two-factor authentication anywhere and everywhere you can.



Data Loss

The inadvertent or malicious loss/exposure of your company data should be a major concern. The ubiquitous nature of online file storage sites make protection of your company's data a more challenging problem than ever to solve. If the loss and/or exposure of your company data is a significant risk for your organization, you have probably already thought about the topic. If data loss and/or data exposure is a lesser risk to your organization, then beware that those with access to data on your network and access to their personal online storage site may be able to easily export your data without your knowledge.

You can help protect your business from Data Loss by following these BEST PRACTICES:

- Identify what is your sensitive data and where your sensitive date is stored.
- Implement web-filtering solutions to restrict access to online file storage and web-based email.
- Restrict the use of USB storage devices.
- Monitor points of egress (internet and email) for sensitive information.
- Audit and limit access to sensitive information.
- Consider the use of encryption for data at rest and in transit.

Section 3: Your Responsibilities

Bank-mandated operational requirements

Your responsibilities as a Bar Harbor Business Online customer should not be taken lightly. They are meant to protect your business.

- The Bank expects that you will provide a computer, software, connections, and equipment as needed to access the Cash Management Services. Your Cash Management Services Master Agreement refers to all of the preceding collectively as "the Computer."

- You are the "Customer." The Customer is responsible for the installation, maintenance, and operation of the Computer and to verify the security of the Computer.

- The Customer is strictly responsible for establishing and maintaining procedures to safeguard against unauthorized instructions, requests, transactions, or transmissions.

- The Customer agrees to adopt and implement its own commercially reasonable policies, procedures, and systems to provide security to information being transmitted and to receive, store, transmit, and destroy data or information in a secure manner to prevent loss, theft, or unauthorized access to data or information ("Data Breaches").

- The Customer is responsible for monitoring their use of all Cash Management Services provided by the Bank, including each transaction processed by the Bank, and notifying the Bank of any errors or other problems.

What if I suspect something is wrong?

Knowing what to do if you suspect unauthorized transactions have occurred or may occur is critical to mitigating potential losses. Contact the Bank if unauthorized transactions have occurred or may occur. Identification and detection of unauthorized transactions require regular monitoring of account activity. This is a responsibility that you must agree to as part of your enrollment in our services. The right course of action will be dictated by the situation. Each situation is different and you may need to engage your technology or service providers to assess the scope of the incident. In addition to contacting the Bank, some or all of the following may be appropriate depending on the situation:

- Change Bar Harbor Business Online password
- Contact service providers regarding forensic investigations, evidence preservation, and subsequent cleanup of impacted computer systems
- Notify law enforcement and attorney general as required by law
- Reinstall the impacted computer system
- Implement additional security controls

The Bank will disable the Cash Management user accounts which have or may have been compromised. In some situations, the Bank will delete your existing bank accounts and create new accounts and/or freeze available funds. The Bank will await confirmation from you that the compromised system or accounts have been cleaned or recovered before reactivating the user account. In some cases, it may be necessary to close the existing accounts and open new accounts.

Section 4: The Bank is Your Partner in Security

The Bank has implemented robust procedural and technical controls to secure the Bar Harbor Business Online environment.

- The Cash Management agreement between your business and Bar Harbor Bank & Trust establishes a trusted employee of your business to be the Cash Management administrator. This is a highly privileged role as the employee is able to assign privileges to manage the cash assets of your Business. The Bank provides dual control for the cash management administrator and must approve any new users or changes to the entitlements of existing users. The Bank will follow up with your designated Cash Management administrator to ensure the changes have been properly authorized.

- Bar Harbor Bank & Trust defines maximum ACH limits for users to prevent users, including the designated Cash Management administrator, from exceeding defined limits. The Bank performs callback authentication to your company telephone number upon receipt of a wire transfer request in excess of $75,000. The customer can request a lower threshold if required.

- The Bank's configuration dictates your company administrator receives an email notification of all ACH and wire transactions initiated by your organization's users.

- Bar Harbor Bank & Trust employs front- and back-line to deliver online banking services to your business. Our Treasury Sales team ensures you get the right services. The partnership between you and the Bank is a mutually binding agreement and the Bank's Cash Management support team ensures the documentation is thorough and complete and gets your Cash Management operation up and running.

- Specific regulatory requirements with regard to Remote Deposit Capture dictate that the Bank inspects your physical site before services are installed. These inspections may be required to be performed annually. The goal of an inspection is to ensure that a proper operating environment is in place to protect your business. The inspection will ensure that the Computer is physically and logically secured to protect from unauthorized exposure and malicious threats.

- Multifactor authentication is required for Cash Management user log-on. The Bank has subscribed to services to ensure that your users are authenticated based not solely on something they know, their password, but also on something they have, their token. Passwords work for anyone who knows or can figure out what they are. The additional token factor makes it many times more difficult to gain unauthorized access to the user account.

- Additional technical controls
  - Challenge questions for suspect log-ins and transactions. Businesses with Cash Management are provided hardware or software tokens for multifactor authentication for log-ins and transactions.
  - Regular email address updates so alerts can be quickly delivered to help customers detect unauthorized activity.
  - Individual user accounts managed by the business to provide for accountability. (Cash Management only)
  - A personal security image chosen by you during account setup assures you the system is authentic.
  - Risk-driven authentication prompts for log-ins and payment actions determined to be high risk. The following factors are evaluated to derive the risk of a log-in or transaction:
    - Browser fingerprints
    - Device cookie
    - Dollar amount payment thresholds
    - New or changed ACH or Wire payment data
    - Algorithm-calculated payment risks
  - iPay fraud alert algorithms and analysts alert the Bank to suspicious Bill Payment activities.

Specifically for Your Bar Harbor Business Online Cash Management

This section provides a detailed list of recommended/optional security controls specific to Bar Harbor Business Online and Cash Management products.

- **Implement time restrictions for Wire and ACH transactions**
  Processing of transactions for your business should occur during expected time frames. If an attacker is able to gain access to your accounts, they may attempt transactions outside of the expected time. This is an opportunity to prevent loss.

- **Implement segregation of duties for any Wire, ACH, and business bill payment processes**
  Establishing dual controls over sensitive processes by segregating duties across multiple personnel ensures no single employee has too much capability. This can protect your assets from insider threats. However, this does require an adequate number of staff to perform the process under a dual control environment. Dual controls are enforced by limiting an employee's entitlements. Ideally, your business will have a Cash Management administrator that is responsible solely for administration. The administrator does not perform transactional functions. Two additional employees are then needed to carry out the business processes.

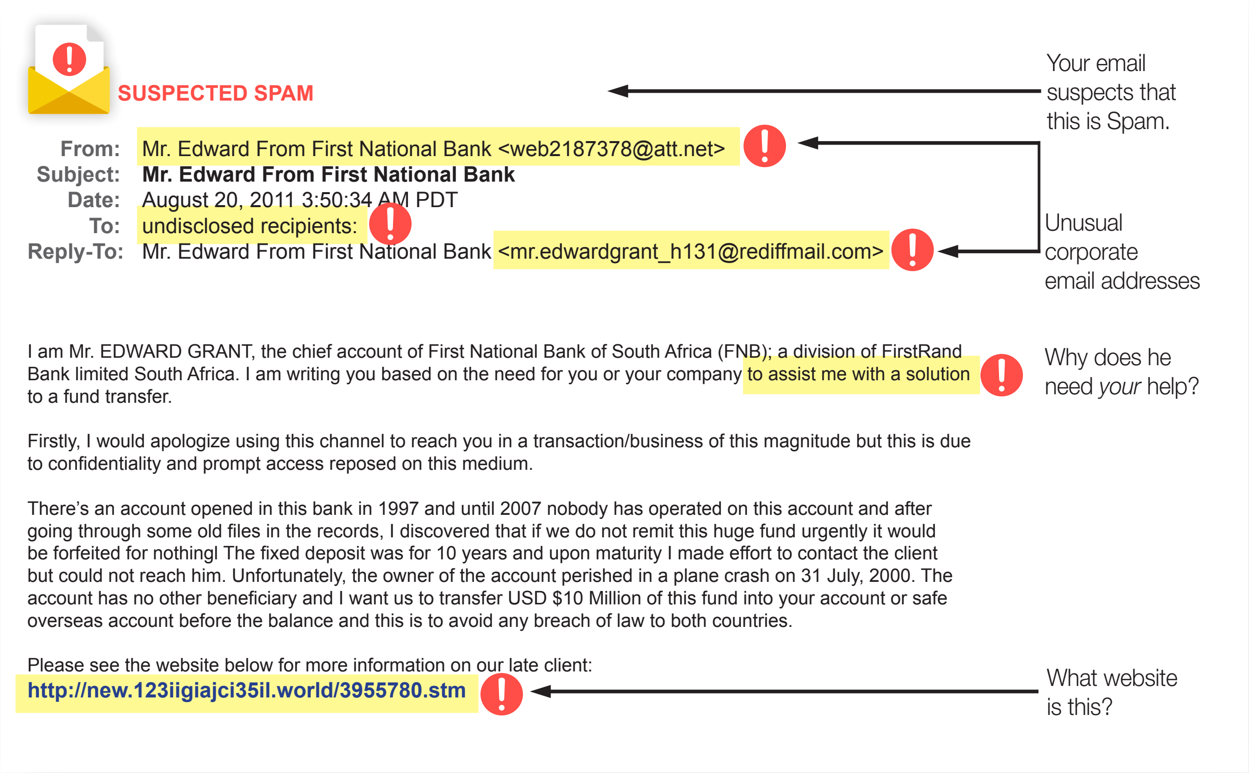
  The following duties are suggested for segregation:
    - Cash management administrators are solely responsible for administering users and do not perform ACH, Wire, or Bill Payment tasks.
    - Add & Edit ACH batches should be segregated from Initiate ACH batch.
    - Add & Edit Wire transfers should be segregated from Transmit wire transfers.
    - Add & Edit Bill Payment payees and payments should be segregated from Initiate payments.

- **Monitor account transactions daily**
  The sooner you identify unauthorized transactions on your account the better. Notify the Bank as soon as possible. It is your responsibility to establish effective operational processes for verifying all transactions on your accounts are authorized.

From external threats

The following best practice controls can help protect your company from email and web-based threats. Deploy multiple lines of defense: use as many as possible!

- Ensure employees are mandated to take security awareness training.
  - Make employees aware that 43% of data breaches start with an employee falling victim to a social engineering attack, most commonly Phishing. (Verizon, 2017)
  - Teach skills for detecting phishing email messages.
  - Make certain employees understand email can be spoofed and may not be from who it claims to be from.
  - Teach mouse-over technique for identifying the actual linked site, not just the link text.
- Avoid web browsing or checking email on computers used for sensitive operations.
- The “Computer” should be dedicated solely to Bar Harbor Business Online processes and not used for other activities.
- Avoid using a privileged system administrator account for routine tasks such as checking email or web-browsing.
- Enable automatic updates for your operating system and third-party applications, especially Microsoft Office suites, Oracle’s Java, and Adobe products.
- Have a competent security firm run a network penetration test and remediate their findings.
- Install antivirus software on your computer and be sure it is updated. Windows Defender is provided free of charge with the Windows operating system.
- Do not disable the security features of your web browser or Office applications. Be cognizant of unexpected warnings or prompts to “enable content.”
- Use a web-filtering system with a reputable URL category database. A regularly updated URL filter database can block access to many thousands of compromised websites.
- Use an email-filtering system to block spam and phishing messages from employee email inbox.
- Back up data regularly and store it somewhere safe. Make sure you can restore from your backup data.
- Ensure mobile devices are running current operating system release versions.
- Ensure employees enable passwords or biometric locks and encryption on their mobile devices. If they are using them for conducting business, your business could be at risk.



SUSPECTED SPAM

From: Mr. Edward From First National Bank <web2187378@att.net>
Subject: **Mr. Edward From First National Bank**
Date: August 20, 2011 3:50:34 AM PDT
To: undisclosed recipients:
Reply-To: Mr. Edward From First National Bank <mr.edwardgrant_h131@rediffmail.com>

I am Mr. EDWARD GRANT, the chief account of First National Bank of South Africa (FNB); a division of FirstRand Bank limited South Africa. I am writing you based on the need for you or your company to assist me with a solution to a fund transfer.

Firstly, I would apologize using this channel to reach you in a transaction/business of this magnitude but this is due to confidentiality and prompt access reposed on this medium.

There’s an account opened in this bank in 1997 and until 2007 nobody has operated on this account and after going through some old files in the records, I discovered that if we do not remit this huge fund urgently it would be forfeited for nothingl The fixed deposit was for 10 years and upon maturity I made effort to contact the client but could not reach him. Unfortunately, the owner of the account perished in a plane crash on 31 July, 2000. The account has no other beneficiary and I want us to transfer USD $10 Million of this fund into your account or safe overseas account before the balance and this is to avoid any breach of law to both countries.

Please see the website below for more information on our late client:
http://new.123iigiajci35il.world/3955780.stm

Your email suspects that this is Spam.

Unusual corporate email addresses

Why does he need *your* help?

What website is this?

From internal threats

The following controls can help protect your business from internal threats. Again, deploy multiple lines of defense.

- Avoid using a privileged system administrator account for routine tasks, such as checking email or web browsing.
- Restrict administrative access to technical staff.
- Keep an inventory of software and identify and eliminate unnecessary software.
- Ensure operating systems and software are supported and up to date.
- Develop procedures with checks and balances for critical or sensitive business operations:
    - Dual controls where possible
    - Segregation and/or rotation of duties
- Disable removable storage auto-run features to prevent infections from infected devices (i.e., USB flash drives).
- Do not allow guests on your business network.
- Have a competent security firm run a network vulnerability assessment and remediate their findings.
- Review the security practices of your technology and service providers.
- Implement monitoring programs for both security and sensitive operations.

Useful Resources

- https://www.stopthinkconnect.org/resources/preview/technology-checklist-for-businesses
- Consider Cyber Liability Insurance: "This is one of the best backup lines of defense small business owners can invest in," says Ted Devine, CEO, Insureon. "Often available to businesses as a rider to a general liability policy, cyber liability insurance can cover costs, including credit monitoring services and investigation fees, when a virus or hacker breaches a business's defenses and exposes customer data."
  https://www.cio.com/article/3186269/cyber-attacks-espionage/how-to-fend-off-cyberattacks-and-data-breaches.html?page=2

Useful Charts/Images

URL malware rate by industry: Malware destined for organizations in the Construction industry had the highest rate of malware in links vs. attachments, with 27.2 percent of malware comprising a link instead of any attachment.

Rank	Industry	% of Email Malware
1	Construction	27.2
2	Ag, Forestry, Fishing	21.5
3	Retail Trade	19.4
4	Finance, Insurance, Real Estate	16.6
5	Mining	13.3
6	Public Admin	11.6
7	Transportation & Public Utilities	11.5
8	Services	10.6
9	Manufacturing	9.5
10	Nonclassifiable Establishments	9.5
11	Wholesale Trade	91

Phishing rate by industry: Many types of industry had phishing rates that were much higher than the global average, with the highest rate for organizations in the Agriculture, Forestry, and Fishing sectors.

Rank	Industry	1 in
1	Ag, Forestry, Fishing	2,212
2	Nonclassifiable Establishments	2,240
3	Public Admin	2,418
4	Mining	2,453
5	Services	2,737
6	Finance, Insurance, Real Estate	3,013
7	Manufacturing	3,998
8	Retail Trade	4,353
9	Wholesale Trade	4,406
10	Construction	4,667
11	Transportation & Public Utilities	5,567

Source: Symantec, 2018

Glossary of Terms

Antivirus — software that protects your computer by detecting and blocking known malware and suspicious behaviors.

Challenge questions — generally a series of knowledge-based questions collected during account setup and used as a secondary means to verify your identity.

Cloud — internet-based services that are typified by being synchronized and highly available and accessible from various platforms including computers and mobile devices.

Control — measures taken to reduce the risk of a threat.

Data breach — the exposure or theft of sensitive information.

Drive-by download — a hidden element on a website and downloads possibly malicious programs to your computer without your knowledge.

Encryption — the process by which data is converted from a readable clear text to cipher (code) text to warrant it unreadable by third parties.

Hacking — the act of attempting to bypass or circumvent computer security controls to gain access to systems or user accounts.

Internet — the global network hosting the World Wide Web, email, and many additional services.

Internet of Things (IOT) — refers to the growing number of commercial and domestic products that are connected to the internet to afford greater control, integration, convenience, etc. (i.e., smart TVs, surveillance cameras, automation devices, environmental and health monitors, etc.).

Malware — computer software that has malicious intent including viruses, trojans, spyware, worms, etc.

Multifactor authentication — a method of confirming a user's claimed identity in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is). (Wikipedia)

Network penetration test — a test of a computer network and the attached systems used to identify vulnerabilities that may be susceptible to attack by outsiders. Historically, penetration tests targeted assets that were accessible from the internet, but today are regularly conducted from networks internal to an organization.

Network vulnerability assessment — a test of a computer network and attached systems used to identify vulnerabilities and configuration weaknesses. Typically, a vulnerability assessment is conducted with full access to the systems so that all known software vulnerabilities and specific configurations can be assessed accurately.

Password guessing — the act of attempting to log-in to a user account by guessing the password. Password guessing is performed online and may lock out user accounts if the authentication system has user account lockout enabled.

Password hash cracking — the act of attempting to infer a password by comparing the hash of a possible password value to stolen password hashes. Password hash cracking is an "offline" attack in which the attacker has already stolen the password hashes from an authentication system. Password hash cracking cannot be thwarted by account lockout or detected by the system under attack.

Password manager — assists in generating and retrieving complex passwords, potentially storing such passwords in an encrypted database or calculating them on demand. (Wikipedia)

Password spraying — a modern "online" password guessing attack in which attackers try to use common passwords across many user accounts. Password spraying allows the attacker to threshold their attack and spread it across many user accounts to avoid account lockouts thwarting their attack. Password spraying is successful because many users choose easily guessable passwords.

PCI Merchant Level — All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As (DBA). (https://www.pcicomplianceguide.org/faq/)

Phishing — fraudulent email messages that attempt to entice recipients to open malicious attachments or follow malicious web links to steal user log-in credentials or sensitive information.

Ransomware — ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to the data unless a ransom is paid to the threat actors.

Social engineering — refers to psychological manipulation of people into performing actions or divulging confidential information. (Wikipedia)

Targeted attack — many threats are opportunistic and attack easily detected vulnerable systems. A targeted attack is geared to a specific organization or individual. Because it is targeted, it can be considerably more difficult to detect and may seem much more legitimate.

Threat — any natural or man-made circumstance that could have an adverse impact on an organizational asset. (InfoSec Institute)

Trojan — a malicious computer program which misleads users of its true intent.

Two-factor authentication (2FA) — authentication requiring at least two factors. See Multifactor authentication.

Vulnerability — the absence or weakness of a safeguard in an asset that makes a threat potentially more likely to occur, or likely to occur more frequently. (InfoSec Institute)

Web filter — a network security device that filters web traffic largely based on categorical blocking of website URLs.

Web request — a single web page may consist of hundreds of individual elements. Your computer makes hundreds of web requests, one for each individual element, to load a single web page.

References

Federal Deposit Insurance Corporation. (Winter 2011/2012). Minding Your Own Business: Banking Tips for Small Companies. *FDIC Consumer News,* 4.

Krebs, B. (n.d.) *Business-email-compromise*. Retrieved April 26, 2018, from KrebsonSecurity.com: https://krebsonsecurity.com/tag/business-email-compromise/

Microsoft. (2017). *Microsoft Security Intelligence Report*. Redmond, WA: Microsoft.

SANS Securing The Human. (2016, July). July 2016 — *The Monthly Security Awareness Newsletter for Everyone*. Retrieved April 26, 2018, from www.sans.org: https://www.sans.org/security-awareness-training/ouch-newsletter/2016/ceo-fraud

Symantec. (2018). Internet Security Threat Report.

Verizon Enterprise. (2017, April 28). *2017 Data Breach Investigations Report*. Retrieved March 26, 2018, from Verizon Enterprise: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Verizon Enterprise. (2016). *Data Breach Digest*. Retrieved April 23, 2018, from www.verizonenterprise.com: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

Vormetric. (2015). *2015 Vormetric Insider Threat Report*. Retrieved April 23, 2018, from vormetric.com: http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

Williams-Grut, O. (2018, April 15). *Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank*. Retrieved April 26, 2018, from businessinsider.com: http://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4

Notes

BAR HARBOR
BANK & TRUST

www.BarHarbor.Bank • 888-853-7100
Member FDIC Equal Housing Lender

Over 50 locations in Maine, New Hampshire, and Vermont

Version – January 2019