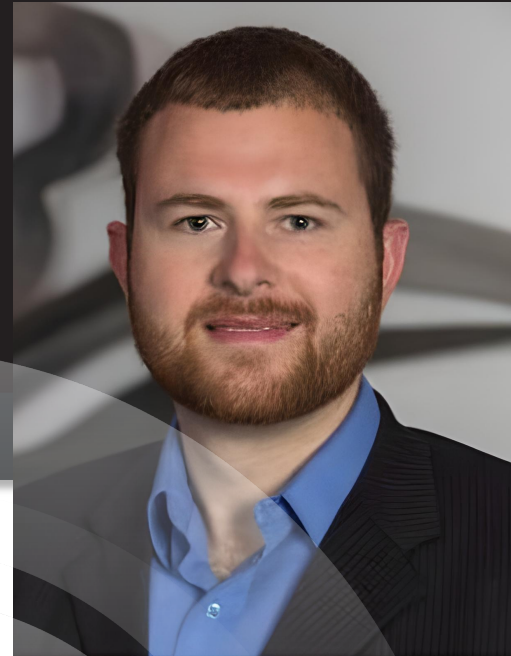




**Security Best Practices from an  
Ethical Hacker's Perspective**

# TIM STEINER

FOUNDER



I have been active in multiple areas of cybersecurity for 15 years and focus on providing commercial and government organizations with realistic and comprehensive cybersecurity strategy. Experience includes organizations from the Department of Defense (DoD) to financial institutions and from Fortune 500 companies to small businesses. Currently I lead technical red team assessments, security architecture reviews, vulnerability assessments, penetration testing, and web application penetration testing.

Certified Information Security Systems Professional (CISSP), Information Systems Security Architecture Professional (ISSAP), Certified Ethical Hacker (C|EH), Offensive Security Certified Professional (OSCP), and holds an M.S. degree in Information Assurance from Wilmington University. Served as the ethical hacking subject matter expert (SME) for Liberty University's School of Engineering and Computational Sciences (2014-2019). Served as former president and founder of the Aberdeen (ISC)2 chapter. Served 20 years in the Air National Guard (Major Retired), was responsible for red team operations during multiple exercises and lead development of offensive cybersecurity training for the state of North Carolina at JFHQ in Raleigh, NC.



## ABOUT CRYPTOTRUST

**About Company:** CryptoTrust was established in 2013 as an independent cybersecurity firm, based in Chatham County, North Carolina that is dedicated to innovating cybersecurity solutions to protect individuals and businesses from cybersecurity attacks and breaches.

### Services

- Vulnerability Assessment
- Penetration Testing
- Cloud Security Architecture Review
- Red Team/Purple Team Exercise

### Products

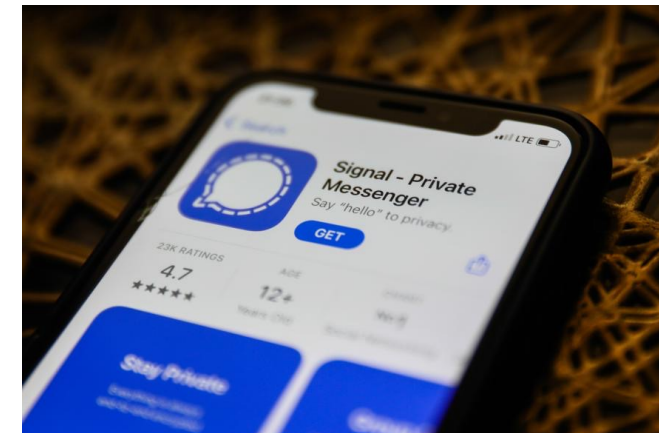
- OnlyKey
- OnlyKey DUO





# WHERE DO WE START?

- Almost anything can be used for hacking and threats are seemingly all around, how can we even know where to start?



# FINDING THE SWEET SPOT

- ❑ There isn't a one size fits all cybersecurity solution.
- ❑ When things are more secure they are less convenient and when things are more convenient they are less secure.
- ❑ Increasing an individual's security almost always means less convenience. I.e. It takes longer to log in with a password and a code sent to your phone then just a password.
- ❑ Increasing an organization's security almost always adds less convenience which translates into real business costs. I.e. It takes everyone longer to log in, they must attend security awareness training, and the company has endless bills for various security products and services.
- ❑ Individuals will only accept a certain level of inconvenience and businesses don't have unlimited budgets so finding balance is key.



## Security vs. Convenience





# DATA DRIVEN CYBERSECURITY

- ❑ Cybersecurity decisions should NOT be based on emotion or opinions of leadership. FEELING vs KNOWING
  - ❑ I.e. The news runs a story on a local government getting hacked, IT manager starts buying solutions they think might help.
  - ❑ I.e. Your friend tells you to never connect to the free Wifi at a coffee shop
  - ❑ Airplane vs. Automobile Travel Safety Example – Does it FEEL safer to fly or to drive?
- ❑ Ensuring a data driven approach to cybersecurity to effectively prioritize and mitigate the most prevalent threats
  - ❑ The threat landscape is a constantly moving target. What worked in the past may not work now, a data driven approach is necessary.
  - ❑ The best data sources for cybersecurity risks come from the risks (threat actors) themselves.



# Understanding top attack methods from recent attacks (MITRE ATT&CK)

- Understanding top attack methods from recent attacks
  - The Mitre Attack Framework - MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
  - Several companies have studied top attack methods and developed a top 10 list (Logpoint, Picus, CrowdStrike, Recorded Future, Red Canary)

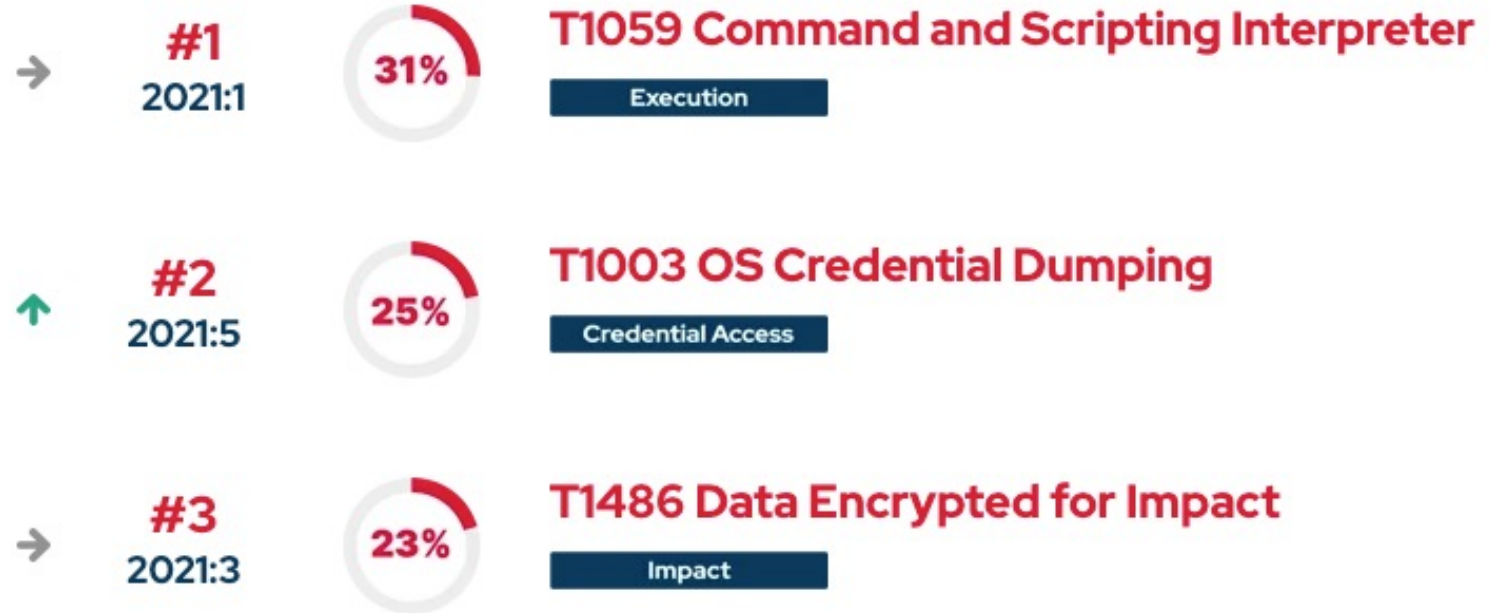
The top 10 lists created by [Picus](#), [CrowdStrike](#), [Recorded Future](#), and [Red Canary](#) are shown in the table below, along with the methodologies used in each list. Different techniques are listed differently, although variety does not imply inaccuracy or incompleteness.

Different findings are expected of the given approaches, and threat samples were utilized to create the lists.

					
1	Command and Scripting Interpreter	Process Injection	Masquerading	Security Software Discovery	Command and Scripting Interpreter
2	OS Credential Dumping	PowerShell	Command-line Interface	Obfuscated Files or Information	Signed Binary Proxy Execution
3	Proxy	Credential Dumping	Credential Dumping	Process Injection	Windows Management Instrumentation
4	Process Injection	Masquerading	PowerShell	System Information Discovery	Credential Dumping
5	Masquerading	Command-line Interface	Hidden Files and Directories	Process Discovery	Ingress Tool Transfer

# Understanding top attack methods from recent attacks (MITRE ATT&CK) cont.

- ❑ Top attack method #1 - The most common technique was T1059 **Command and Scripting Interpreter** which allows for the execution of various commands that directly or indirectly lead to almost every tactic in the list. A whopping 38.12% of incidents we detected were making use of the Command and Scripting technique.
- ❑ Top attack method #2 – T1003 **OS Credential Dumping** is a technique for obtaining account login and password information for the victim's operating system. Once adversaries establish initial access to a system, one of their primary objectives is to find credentials to access other systems and resources in the environment.
- ❑ Top attack method #3 - Crypto-ransomware utilizes encryption algorithms that are practically impossible to break when implemented correctly. According to the MITRE ATT&CK framework, this technique is called T1486 **Data Encrypted for Impact**.





# Understanding top attack methods from recent attacks (MITRE ATT&CK) cont.

- ❑ Demonstration will be conducted to show the top 3 attack methods in action
  - ❑ **T1059 Command and Scripting Interpreter**
    - ❑ User downloads and opens a malicious file that uses a combination of PowerShell, CMD, and VBS to establish command and control of a workstation.
  - ❑ **T1003 OS Credential Dumping**
    - ❑ Attacker dumps credentials that can be used to access other systems.
  - ❑ **T1486 Data Encrypted for Impact.**
    - ❑ Attacker uses admin credential to encrypt files (Crypto ransomware)



# Understanding how attackers chain multiple tactics to achieve objectives

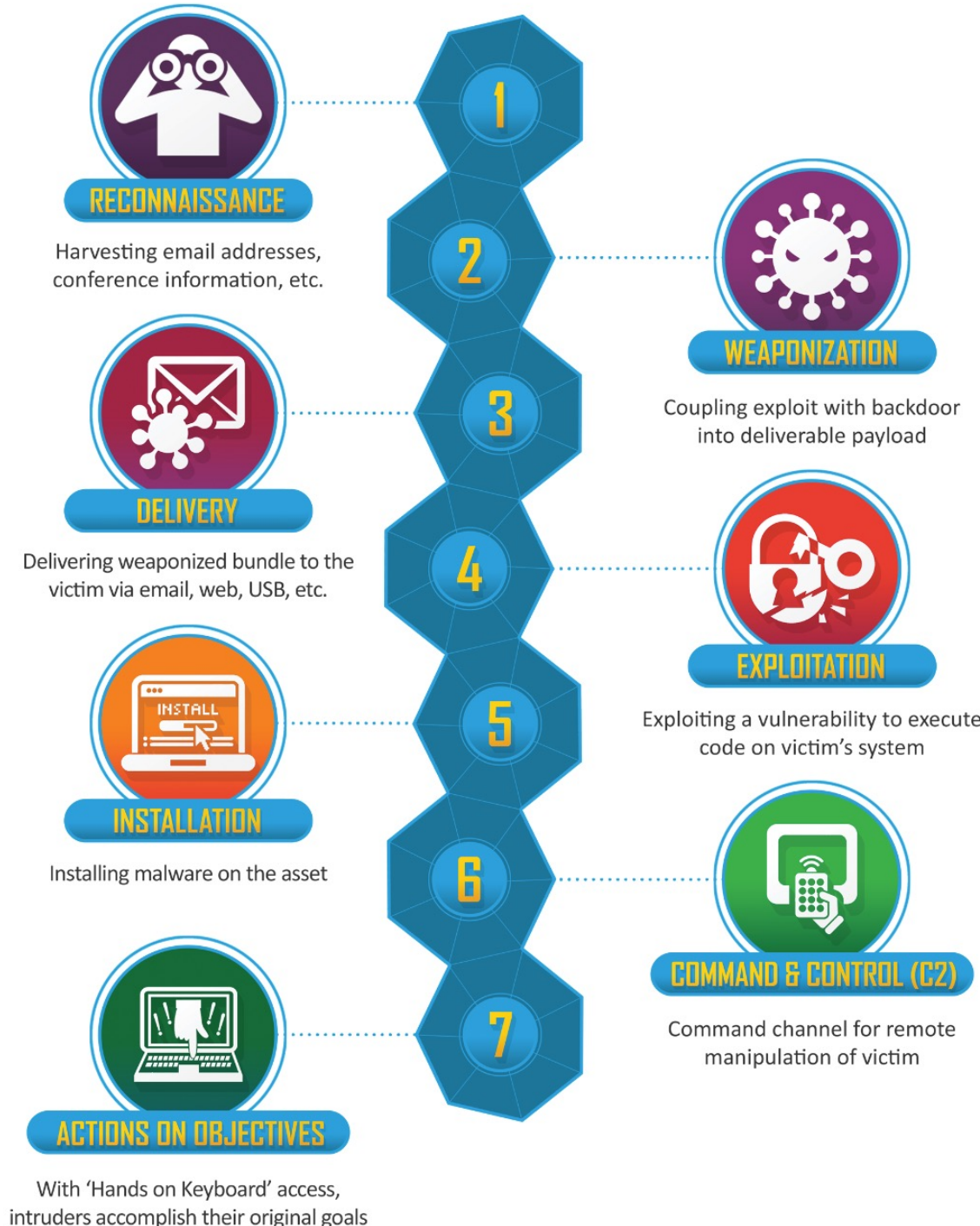
Another model, the Lockheed Martin Cyber Kill Chain® model is shown which accurately illustrates how attackers commonly infiltrate systems.

This can also be mapped to MITRE ATTACK as follows:

T1059 **Command and Scripting Interpreter** - (4) EXPLOITATION

T1003 **OS Credential Dumping** - (7) ACTIONS ON OBJECTIVES – Here the adversary objective is to obtain credentials/passwords to access more systems and data.

T1486 **Data Encrypted for Impact** - (7) ACTIONS ON OBJECTIVES – Here the adversary objective is to encrypt data in order to force payment of a ransom to get that data back





# Developing defenses to threat tactics

- ❑ Understanding a threat through modeling
  - ❑ For a business, what are my crown jewels of the business?
  - ❑ For an individual, what is my most important data?
- ❑ Look at worst case scenarios through the lens of CIA (Confidentiality, Integrity, and Availability)
  - ❑ The same data may have different worst case scenarios based on business and context.
  - ❑ I.e. For an accounting firm, the confidentiality of client data may be most important.
  - ❑ I.e. For a bank, the integrity of data may be most important
  - ❑ I.e. For a hosting company, availability may be most important



# Other Key Factors to Developing Defenses

- ❑ Developing defense in depth solutions
  - ❑ Solutions should assume that any single solution can fail. Defense in depth with zero trust architecture assumes any single solution can fail.
    - ❑ **Defense in depth** - In the event that adversary gets past one layer of security there should be another layer of security (i.e. if the attacker breaches the network perimeter to access a workstation there is a SIEM that detects anomalous activity on the workstation).
    - ❑ **Zero Trust Architecture** – In the event of compromise the attacker shouldn't have access to everything, a user should not be able to log in once and access everything. This means an attacker that compromises the user could do the same. (i.e. if the attacker breaches the network perimeter to access a workstation that workstation is segmented from other critical areas of the network). Solutions such as Illumio provide zero trust segmentation.





# The essential role of cybersecurity testing in developing defenses

- ❑ Cybersecurity testing and Ethical Hacking identifies gaps in defenses before the bad guys do.
  - ❑ A common penetration test finding/gap is that the organization patched all systems EXCEPT some 3<sup>rd</sup> party vendor systems weren't patched leaving a security gap.
  - ❑ Another common penetration test finding is that MFA was enabled for all users EXCEPT some contractor accounts and maybe other exceptions were made for specific users that had issues.
  - ❑ Exceptions can become the weak link that results in a breach, security testing identifies these gaps before they become a breach.



# Security Best Practices for Individuals Checklist

- ❑ The top things in order of priority individuals can do to protect themselves
- ❑ **#1 Adding 2nd factor, MFA, Authy or Google Authenticator** works well for most users.
- ❑ **#2 Using a software password manager** is recommended by most security experts.
  - ❑ Software password require a VERY good master password and ALWAYS use MFA. MAKE SURE YOU HAVE A BACKUP, don't get locked out of your own accounts!
  - ❑ **ONLINE PASSWORD MANAGERS** (encrypted and stored in the cloud)
    - ❑ **Bitwarden** is currently the solution I recommend for the average user as it has a good balance of usability and security.
    - ❑ Lastpass is the most popular but has had security breaches in the past.
  - ❑ **OFFLINE PASSWORD MANAGERS** (encrypted and stored on computer)
    - ❑ **KeepassXC**
    - ❑ Physical such as **OnlyKey**
- ❑ **#3 Don't download and run any untrusted software** on your PC. Be suspicious about opening documents from others, installing or running anything and ensure it was downloaded from a reputable source such as Microsoft.com.



Other Free Products I Recommend – **Signal Messenger, Bitwarden Send, Brave Browser, Tails, ProtonMail, ProtonVPN, DuckDuckGo, Veracrypt, CryptoMator**



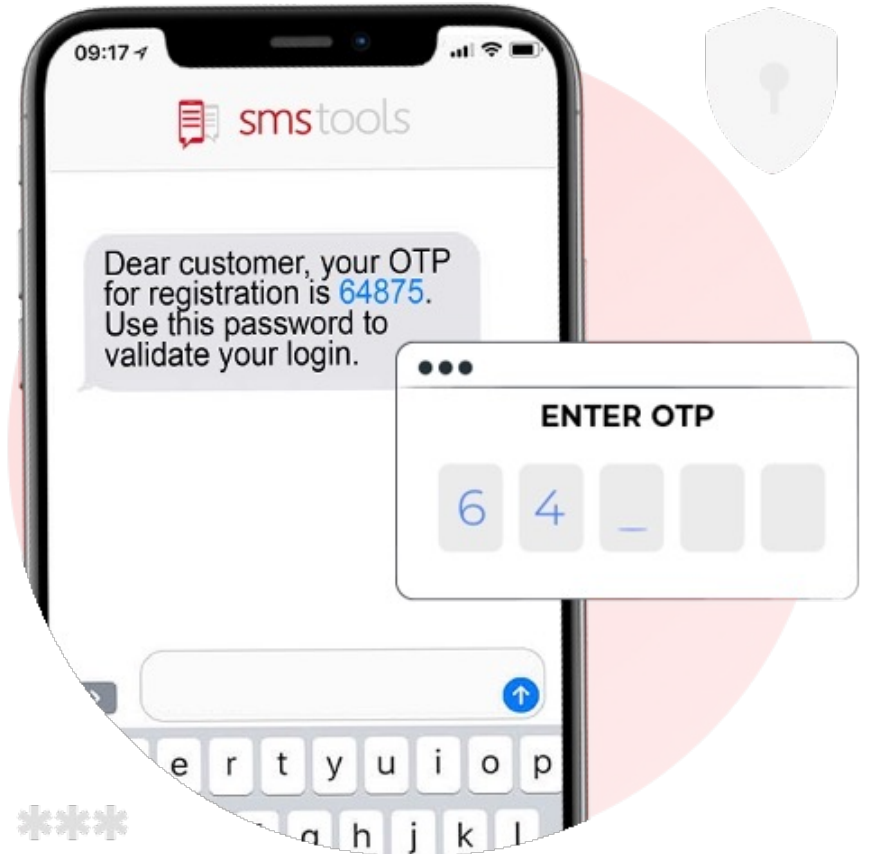
# Security Best Practices for Individuals

- ❑ #1 Adding 2nd factor, MFA, review of what threats apply to certain MFA methods
  - ❑ (BETTER THAN NOTHING) SMS based MFA
    - ❑ SIM swapping (your phone is locked but your SIM can be stolen)
  - ❑ (GOOD) OATH-TOTP (Google Authenticator, Authy, Microsoft Authenticator)
    - ❑ One-time six digit code is only valid for <1 minute, phishing and social engineering may still occur.
  - ❑ (BETTER) Push-app notifications
    - ❑ A user may accept the notification accidentally
  - ❑ (BEST) Physical security keys (FIDO2)
    - ❑ Best solution for security but usability may be an issue



# Security Best Practices for Individuals

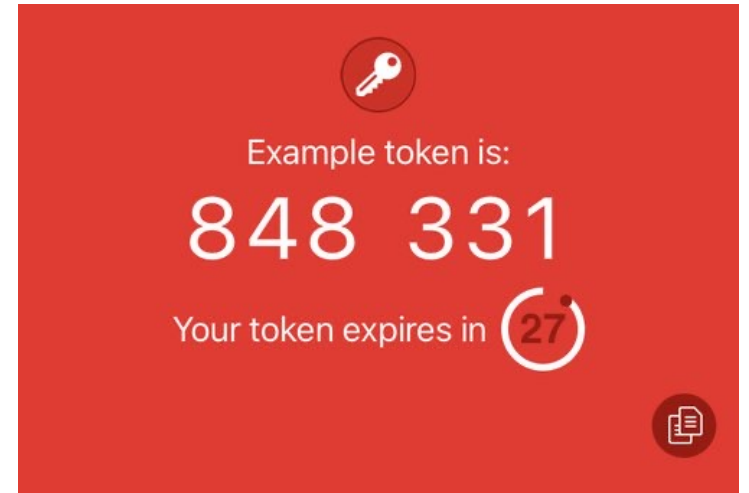
- ❑ SMS based MFA, there are a lot of ways someone can hack SMS based MFA.
  - ❑ Leaving your phone unlocked
  - ❑ SIM stealing (your phone is locked but your SIM can be stolen)
  - ❑ SIM swapping – Your phone service requires knowing a PIN to assign your number to a new phone... Unless -- T-mobile store tablet theft example.





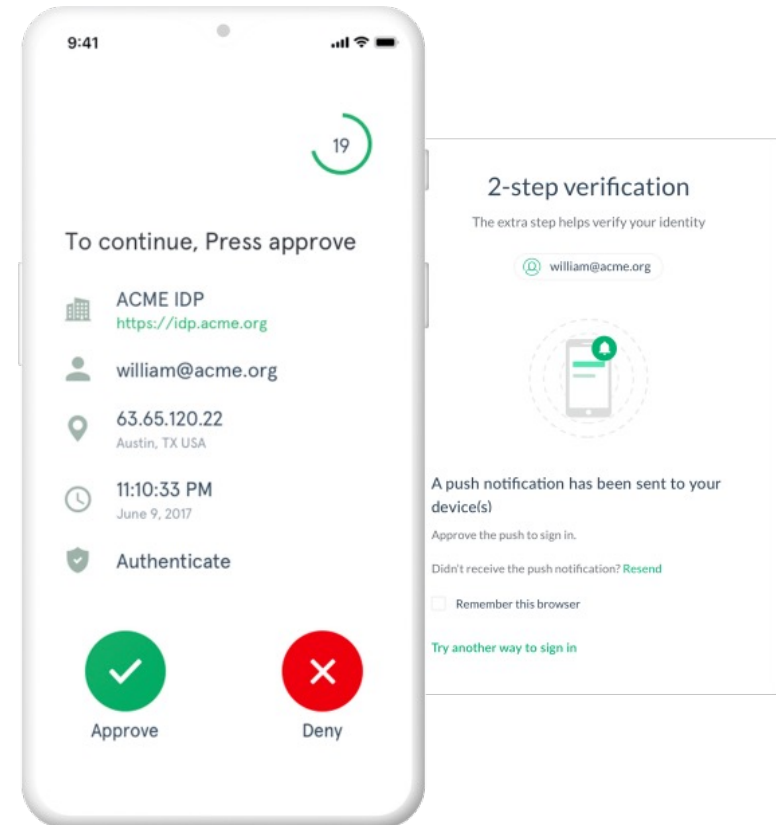
# Security Best Practices for Individuals

- ❑ OATH-TOTP (Google Authenticator, Authy, Microsoft Authenticator) One-time six digit code is only valid for <1 minute
  - ❑ Unlike SMS, the code isn't sent to the phone. It's generated on the phone itself and so harder to hack.
  - ❑ Phishing and social engineering may still occur.
  - ❑ Phone theft/break in may still occur



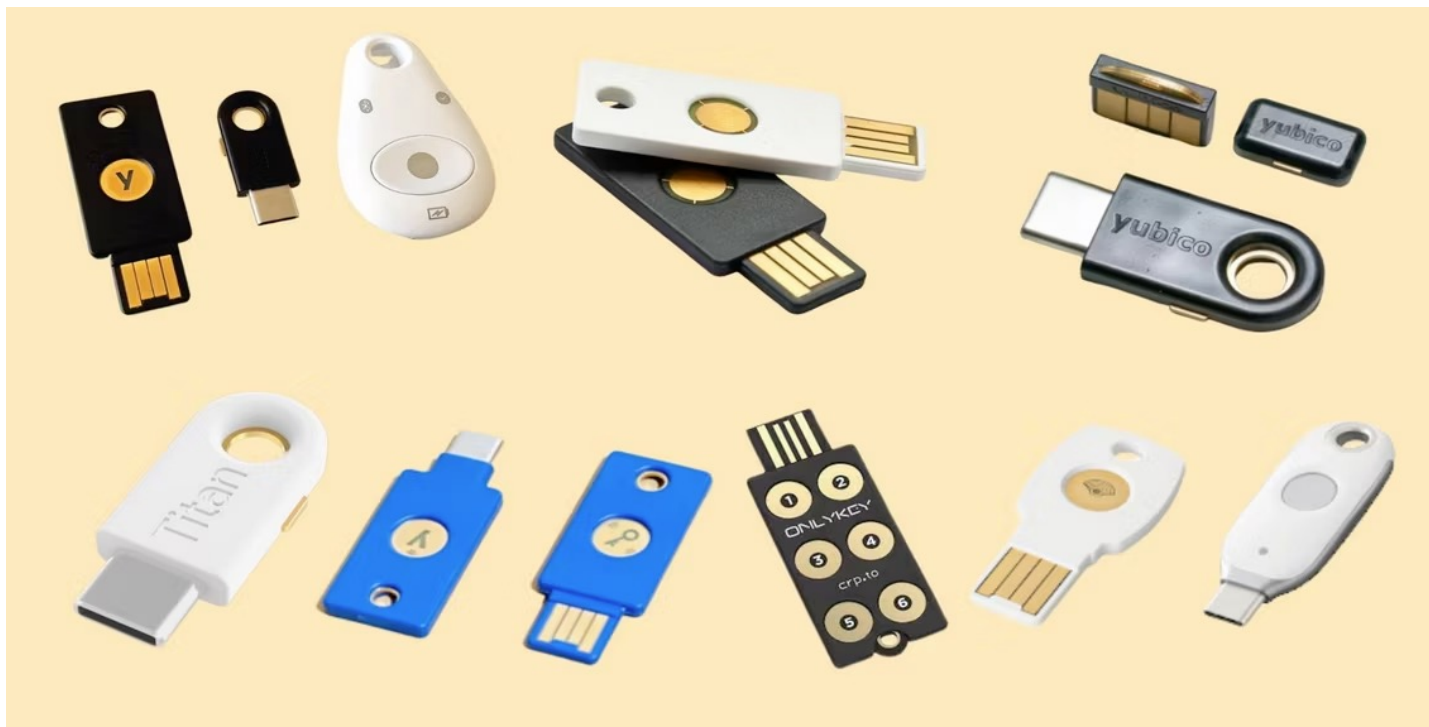
# Security Best Practices for Individuals

- ❑ Push-app notifications
  - ❑ Unlike SMS and TOTP, there isn't a code to hack. It's an approval that the user can read and verify that it is them trying to log in.
  - ❑ A user may still accept the notification accidentally
  - ❑ This method provides the user with additional information on what login they are approving. But in some cases users may not look at or understand and approve an unauthorized login.



# Security Best Practices for Individuals

- ❑ Physical security keys (FIDO2)
  - ❑ Unlike SMS and TOTP, there isn't a code to hack. A physical device cannot be phished.
  - ❑ Unlike Push-app notifications even if the phone is completely compromised the attacker needs the physical security key to log in.
  - ❑ This is the best solution for security but not convenience. Usability may be an issue.
  - ❑ A physical security key is carried by the user and required to login. If the user is prone to losing things this could mean being locked out of account. A secondary backup key or method must be set up to prevent this.

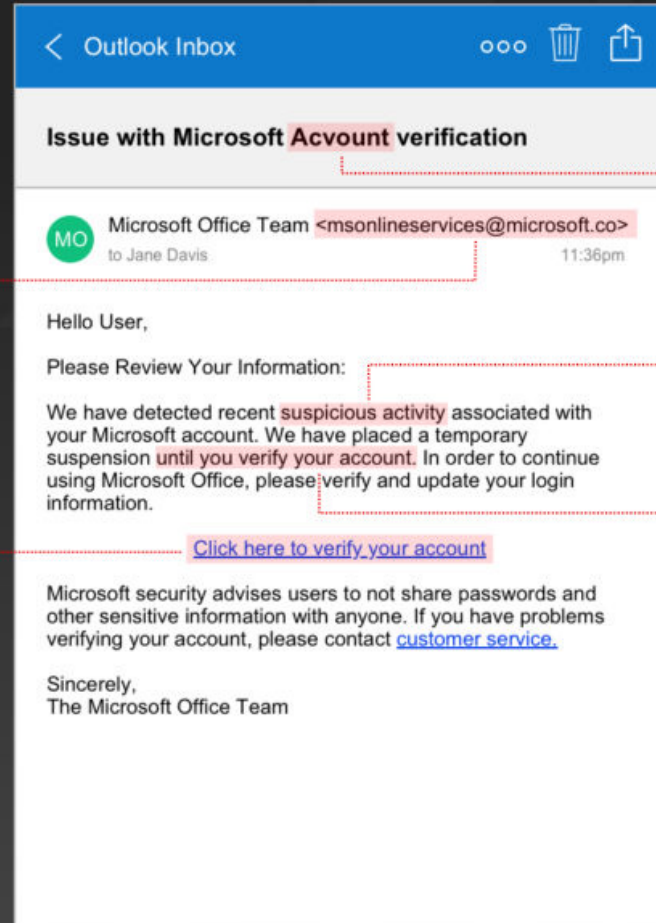


# HOW TO SPOT A PHISHING EMAIL

- ❑ General Rule #1
  - ❑ Never click a link in an email. Most security conscious companies will tell you go to the web site to login to view notification.
- ❑ General Rule #2
  - ❑ If there is an important link you must access do this instead of clicking. Hover over the link, copy the link (usually right click to copy), paste the link into virustotal.com to check if it is malicious. Open a private tab/window in browser and paste link to view.
- ❑ General Rule #3
  - ❑ Never open an email attachment unless you are very sure of the sender and the file type. PDFs are safe most of the time, EXEs or other unknown types are not safe. DOCX and XLSX files are risky.

## PHISHING EXAMPLE

This email is not targeted and fairly generic



Incorrect  
Email

The attacker hides the malicious link behind what appears to be a normal verification button.

Spelling  
Mistake

Attention Grabber

Here, the attacker tries to create a sense of urgency. Before panicking, check to confirm whether this particular email is applicable to your recent activities.



# Security Best Practices for Organizations Checklist

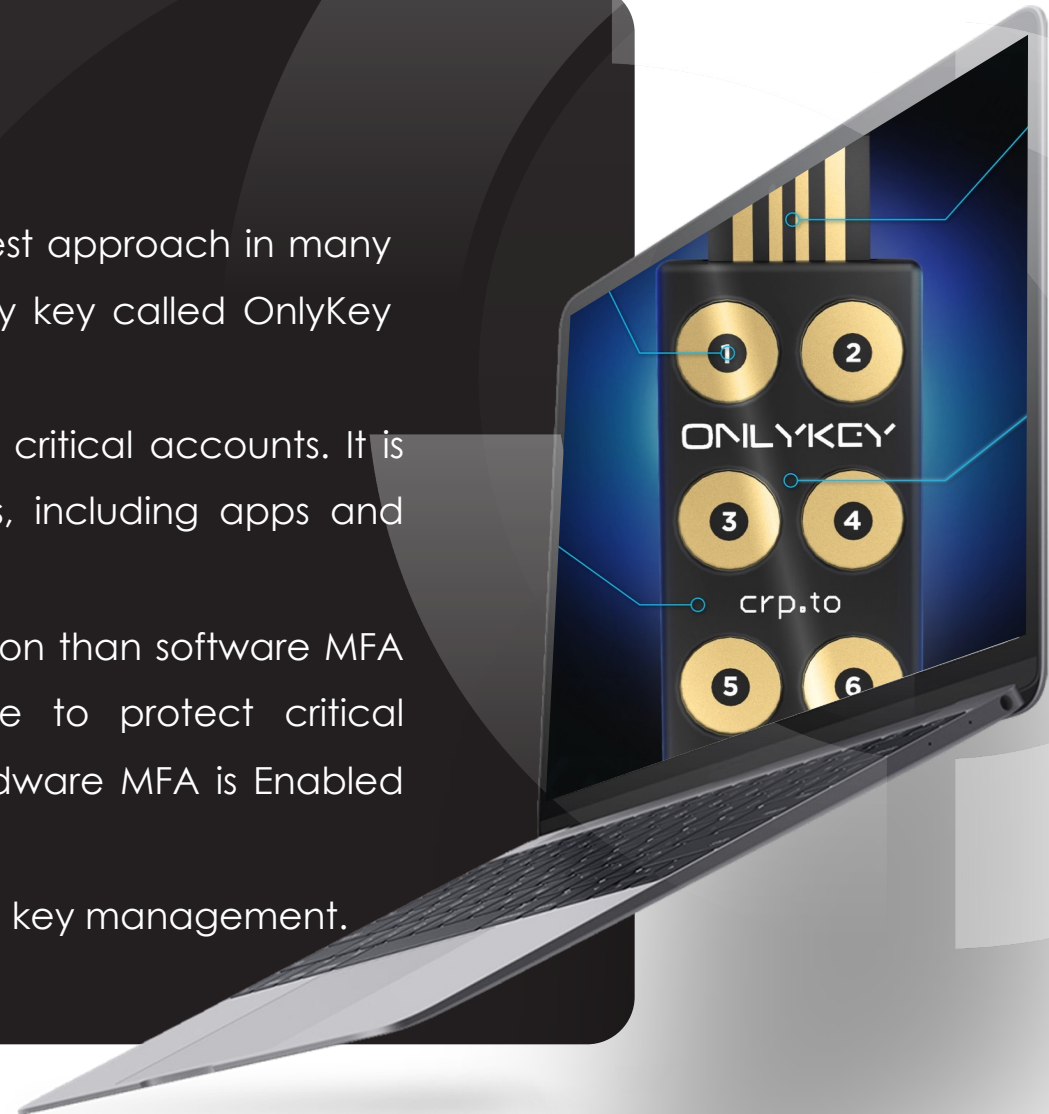
- ❑ **MUST use MFA for critical accounts.** This should always include anywhere Windows domain accounts are used (I.e. VPN or O365 login).
- ❑ Should implement a **next generation EDR/XDR product** on Windows end-points. Endpoints are the most likely to be compromised as demonstrated. AI powered tools such as CrowdStrike and Sentinel One provide better protection than traditional antivirus tools. This should be able to detect **T1059 Command and Scripting Interpreter** and **T1003 OS Credential Dumping**.
- ❑ **MUST have good backups** for many reasons but specifically to mitigate **T1486 Data Encrypted for Impact**. Without good backups some organizations get ransomware and are forced to either pay the ransom or go out of business.
- ❑ Should implement controls to prevent using weak or dictionary based passwords. Windows default settings are not enough as Summer2023! Is considered a strong complex password, but can be cracked by a hacker in no time. 3<sup>rd</sup> party solutions should be implemented to manage and prevent dictionary based passwords.
- ❑ Implement a robust cybersecurity testing program to include regular penetration tests of internal/external/wireless and cloud-based networks. Conduct web application penetration testing on all new web applications before deploying to the public Internet and regularly conduct assessments.



# CRYPTOTRUST ONLYKEY

As we discussed a physical security key is the best approach in many ways to MFA. We developed a physical security key called OnlyKey with these unique features:

- > **Hardware password protection** for business critical accounts. It is compatible with all browsers and devices, including apps and encrypted drives.
- > **Hardware MFA** key provides better protection than software MFA solutions and is required for compliance to protect critical accounts "CIS Benchmark 1.14 Ensure Hardware MFA is Enabled for the Root Account."
- > **Hardware key protection** for business critical key management.



# ABOUT ONLYKEY

OnlyKey is an innovative product developed in Chatham County! It is a patented, proven hardware security key. With no single solution available to address all of a businesses' authentication needs, organizations are left with a fragmented Identity Access Management (IAM) infrastructure. OnlyKey closes the enterprise gap in IAM solutions. As a result, OnlyKey has become a leading authentication/password management solution.



**TRUST THAT YOU CAN TOUCH**  
One thing hackers and malware on a computer cannot do is physically touch something. Your direct physical approval is required to log in.

**EASY LOG IN**  
No need to remember multiple passwords because by plugging OnlyKey to your computer, it automatically inputs your username and password. It works with Windows, Mac OS, Linux, or Chromebook, just press a button to login securely!

**PROTECT ONLINE ACCOUNTS**  
A password manager, two-factor security key, and secure communication token in one, OnlyKey can keep your accounts safe even if your computer or a website is compromised. OnlyKey is open source, verified, and trustworthy.

**PIN PROTECTED**  
The PIN used to unlock OnlyKey is entered directly on it. This means that if this device is stolen, it becomes purposeless, after 10 failed attempts to unlock, data is securely erased.

**PORTABLE PROTECTION**  
Extremely durable, waterproof, and tamper resistant design allows you to take your OnlyKey with you everywhere.





## OnlyKey Background

OnlyKey was created in 2016 to provide a secure hardware platform for password management and MFA in a portable/durable package. As an ethical hacker I regularly conduct tests for clients to identify security flaws and when I hear they use a software password manager I know that all I have to do is compromise one computer and then I will be able to access every account the user has. From a hacker perspective even if everything on a computer may be compromised, a separate physical hardware device is not. By storing passwords on a physical device they can remain safe even if the computer is hacked.





# GET IN TOUCH



## Address

11312 US 15-501 North  
STE 107143, Chapel Hill,  
NC 27517



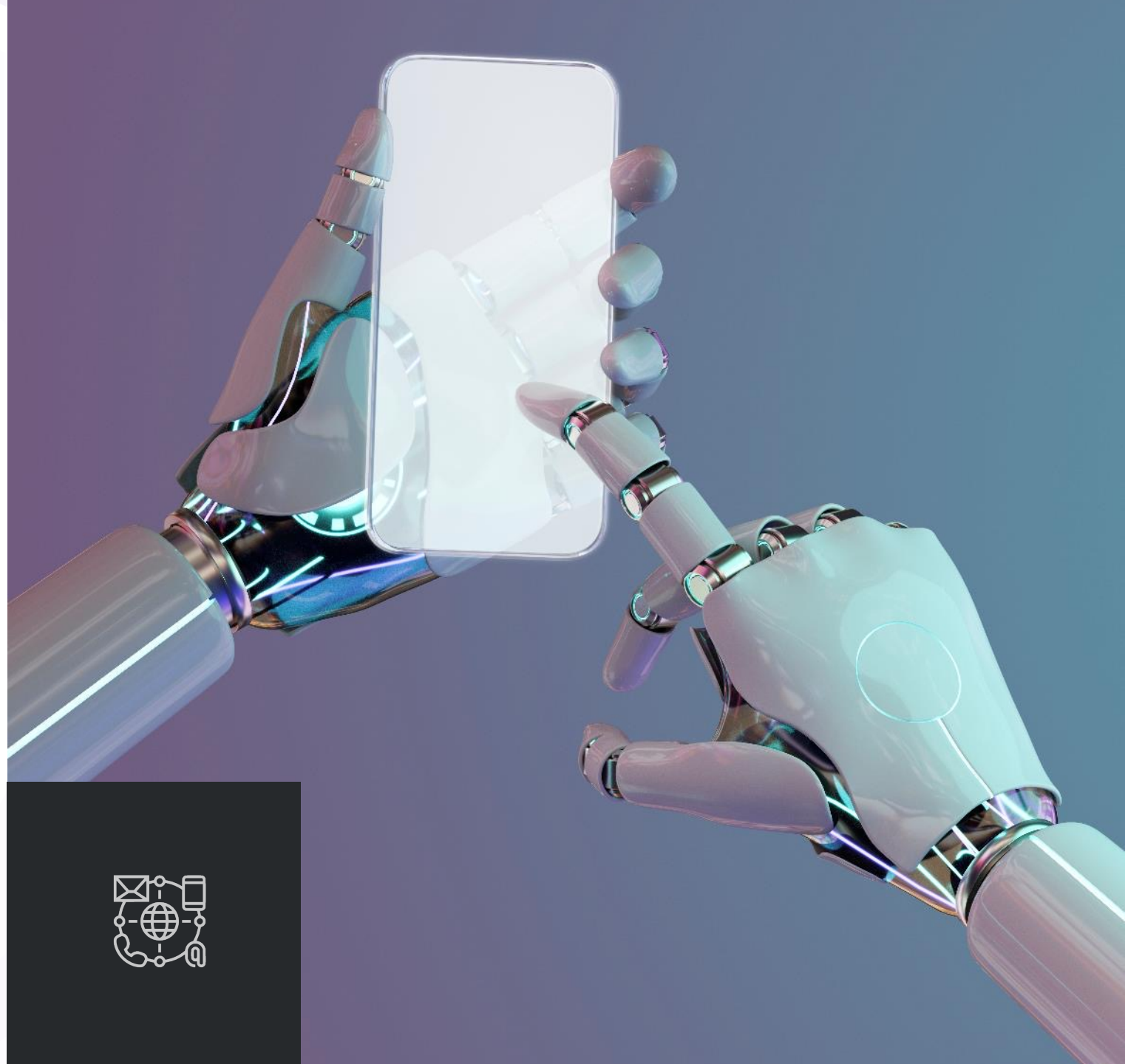
## Email

t@crp.to




## Phone

848.207.4222





**THANK  
YOU**

**ONLYKEY** |  **CryptoTrust**