

KnowBe4
Human error. Conquered.

The Good, the Bad, and the Truth About Password Managers



Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com



Roger A. Grimes

Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com

Twitter: [@RogerAGrimes](https://twitter.com/RogerAGrimes)

LinkedIn: <https://www.linkedin.com/in/rogeragrimes/>

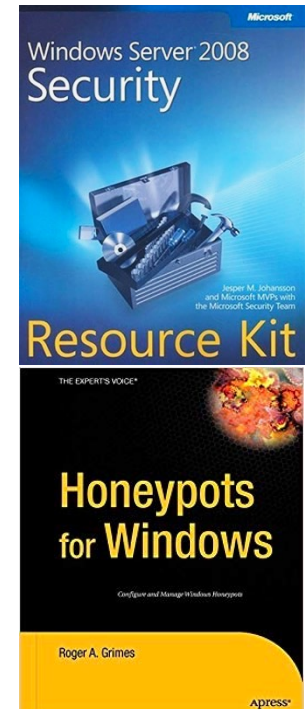
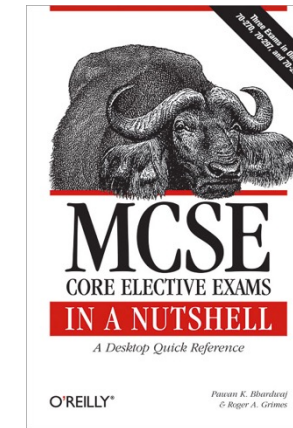
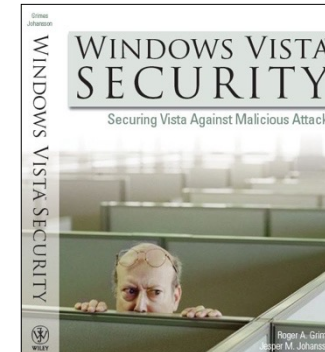
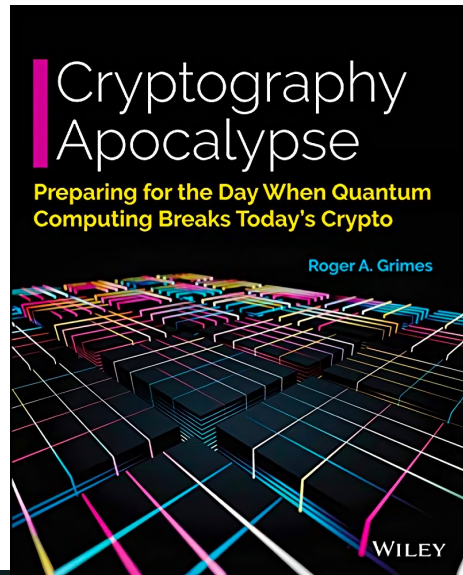
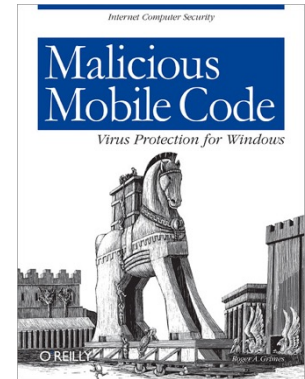
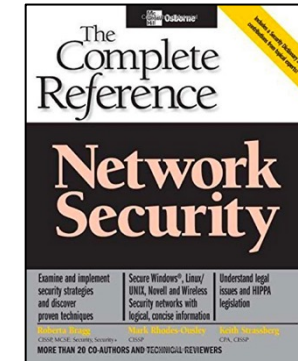
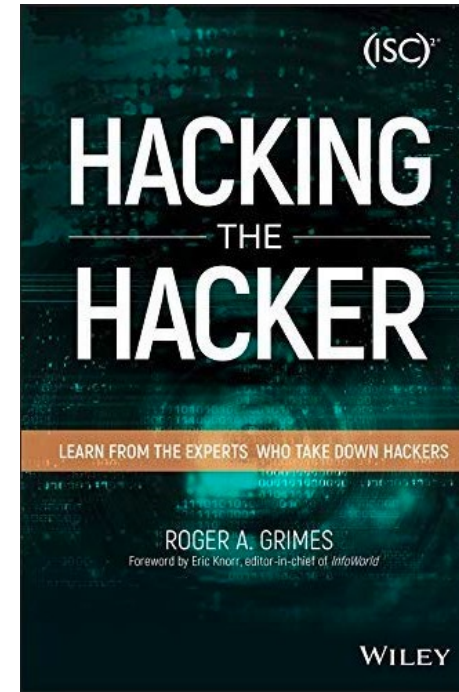
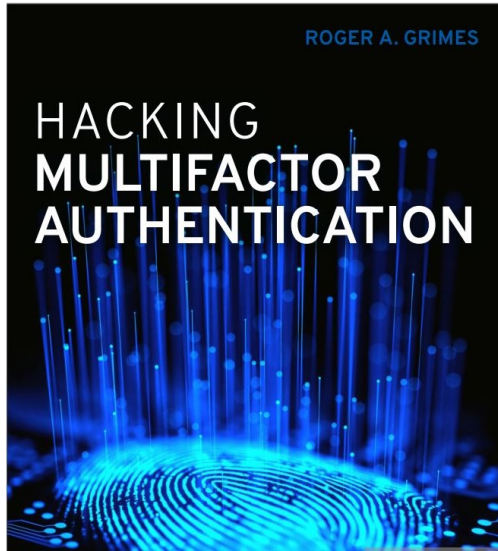
About Roger

- 34 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,200 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certification exams passed include:

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Roger's Books



About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil



Agenda

- Why Use a Password Manager?
- Common Features of a Password Manager
- How Password Managers Can Be Attacked
- How to Best Defend Your Password Manager

Agenda

- Why Use a Password Manager?
- Common Features of a Password Manager
- How Password Managers Can Be Attacked
- How to Best Defend Your Password Manager

Why Use a Password Manager?

Biggest Password Problem and Risk Today

- The average person has to logon to over 170+ sites/services and only has 3 to 19 passwords
- Lots of weak, shared passwords (or password patterns)
- Lots of passwords that are easy for adversaries to guess
- One compromise more easily leads to other compromises

Why Use a Password Manager?

Password Strength

- Most user-created passwords are weak (i.e., low entropy)
- Most are short (10-characters or less)
- Most use predictable “complexity”
- Example: Rogrimes2 or GoBucs2023!
- Better: b0yLoves2JumpOverC@lvEs

Truly random password examples:

- Ac3HEX76cFLtPvXRgQFM
- skYo!YECv2RsoTrAAQcR
- zs88wNoz-zcvPLm!_6H*

Why Use a Password Manager?

Example Real World Password (Hash) Cracking Report

We found that the Department's management practices and password complexity requirements were not sufficient to prevent potential unauthorized access to its systems and data. Over the course of our inspection, we cracked 18,174 of 85,944—or 21 percent of active user passwords, including 288 accounts with elevated privileges and 362 accounts of senior U.S. Government employees.

In the course of our work, we found that:

- The Department did not consistently implement multifactor authentication, including for 89 percent of its High Value Assets (assets that could have serious impacts to the Department's ability to conduct business if compromised), which left these systems vulnerable to password compromising attacks.
- The Department's password complexity requirements were outdated and ineffective, allowing users to select easy-to-crack passwords (e.g., Changeme\$12345, Polar_bear65, Nationalparks2014!). We found, for example, that 4.75 percent of all active user account passwords were based on the word "password." In the first 90 minutes of testing, we cracked the passwords for 16 percent of the Department's user accounts.
- The Department's password complexity requirements implicitly allowed unrelated staff to use the same inherently weak passwords—meaning there was not a rule in place to prevent this practice. For example, the most commonly reused password (Password-1234) was used on 478 unique active accounts. In fact, 5 of the 10 most reused passwords at the Department included a variation of "password" combined with "1234"; this combination currently meets the Department's requirements even though it is not difficult to crack.

https://www.doioig.gov/sites/default/files/2021-migration/Final%20Inspection%20Report_DOI%20Password_Public.pdf

Why Use a Password Manager?

Password Attacks

- Online logon portals often allow hundreds of thousands of guesses without locking attacker out (over the lifetime of the password)
- Password hashes can be guessed at tens of trillions of times a sec
- Most passwords made up by people are guessable within the lifetime of the password, most within hours to days

Akamai: We Saw 61 Billion Credential Stuffing Attacks in 18 Months

- Webinar on password attacks: <https://info.knowbe4.com/password-masterclass>

Why Use a Password Manager?

Biggest Password Problem and Risk Today

- Hackers can often just guess at people's passwords

Bill said he's not sure where the passwords are coming from, but he assumes they are tied to various databases for compromised websites that get posted to password cracking and hacking forums on a regular basis. Bill said this criminal group averages between five and ten million email authentication attempts daily, and comes away with anywhere from 50,000 to 100,000 of working inbox credentials.

In a December 2020 blog post about how Microsoft is moving away from passwords to more robust authentication approaches, the software giant said *an average of one in every 250 corporate accounts is compromised each month*. As of last year, Microsoft had nearly 240 million active users, according to this analysis.

From: <https://krebsonsecurity.com/2021/09/gift-card-gang-extracts-cash-from-100k-inboxes-daily/>

Why Use a Password Manager?

Biggest Password Problem and Risk Today

- There are hundreds of password “dumps” with billions of stolen passwords

';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) **pwned?**

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

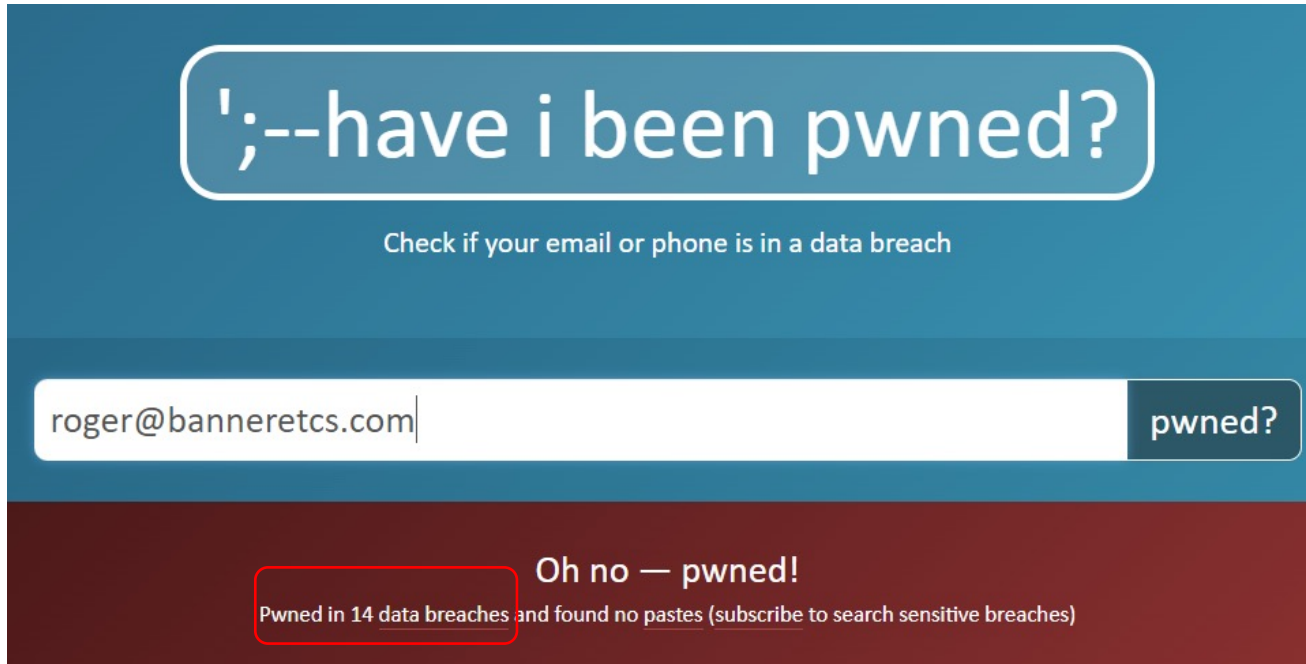
[Why 1Password?](#)

646	12,441,647,441	115,580	227,246,091
pwned websites	pwned accounts	pastes	paste accounts

Why Use a Password Manager?

Biggest Password Problem and Risk Today

Here's how many times my passwords have been knowingly compromised:



Password Compromises Include:

- Facebook.com
- Twitter.com
- Diet.com
- Mgm.com
- Citibank.com
- Experian.com
- Govconnect.com
- My healthcare provider

None of these were due to anything I did – the site I belonged to was breached

Password Hash Cracking

How Fast Can Password Hashes Be Cracked?

Password hash cracking speed on 45TH/s rig against perfect random passwords

Hash	Eff. Speed	Password Length							
		6	7	8	9	10	11	12	
LM	15.81 TH/s	instant	instant	instant	instant	instant	instant	instant	
NT	31.82 TH/s	instant	instant	3.5 min	5.5 hrs	3 wks	5.6 yrs	538 yrs	
MD5	17.77 TH/s	instant	instant	6 min	10 hrs	9 wks	10.1 yrs	963 yrs	
SHA1	5.89 TH/s	instant	instant	19 min	29 hrs	15 wks	30.6 yrs	2.9M yrs	
SHA2-256	2.42 TH/s	instant	instant	45.5 min	3 days	37 wks	74.25 yrs	7.1M yrs	
SHA2-512	801.9 GH/s	instant	instant	2.25 hrs	9 days	28 mon	225 yrs	21.4M yrs	
BCRYPT	11.37 MH/s	18 hrs	9 wks	59 yrs	5.6M yrs	534M yrs	50744M	4820555M	

Data from: <https://t.co/NKYIrKwUDb>

This is why you need 12-character perfectly random passwords

Why Use a Password Manager?

Password Strength

- Almost all passwords made up by people are guessable within the lifetime of the password, most within hours to days
 - 12-character perfectly random password is unguessable/uncrackable
 - User created password needs to be 20-char or longer to be unguessable/uncrackable
-
- Webinar on password attacks: <https://info.knowbe4.com/password-masterclass>

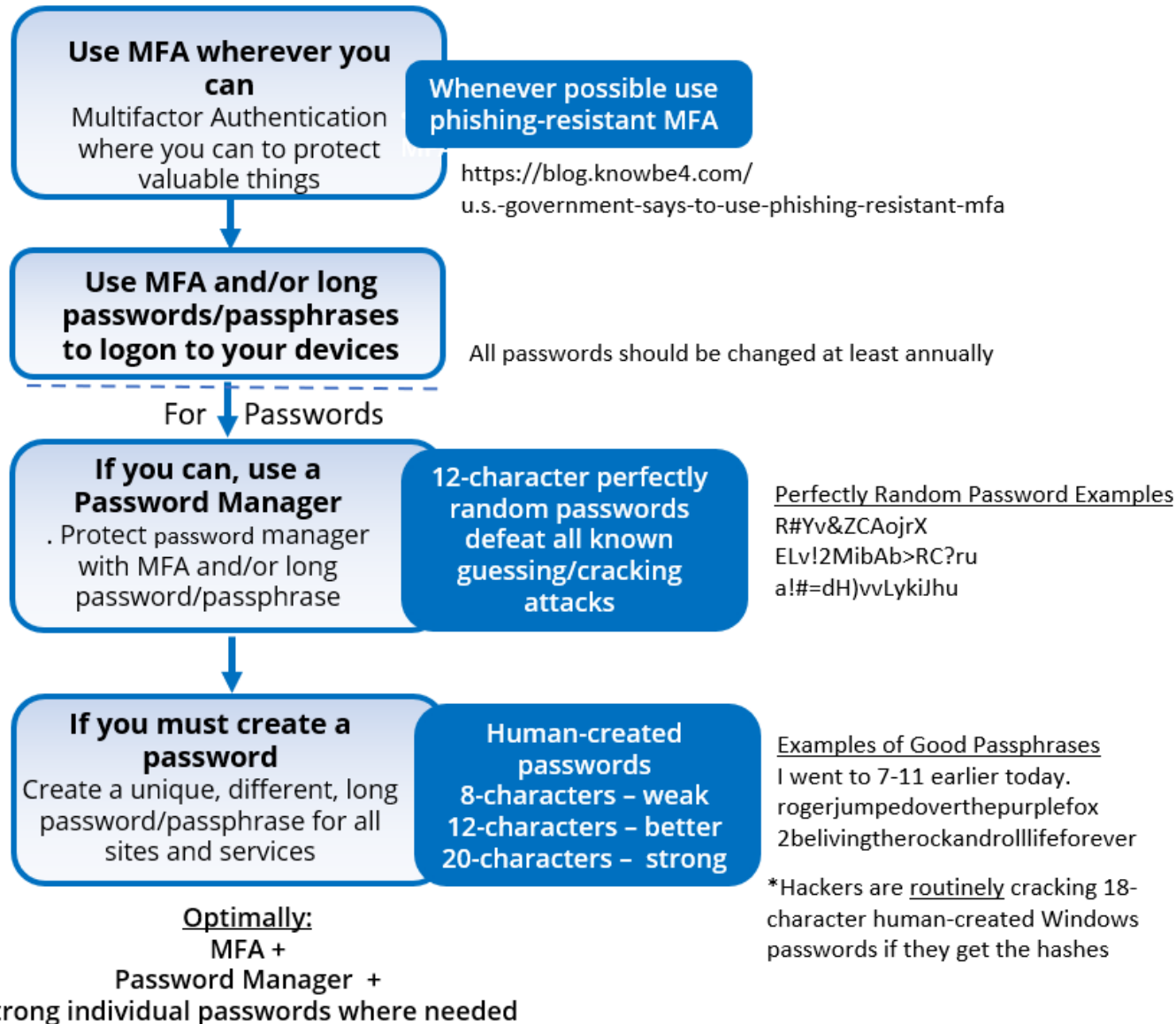
Why Use a Password Manager?

Major Benefits of a Password Manager

- Allow you to create and easily use unique, strong, perfectly random passwords for each site/service
- Can easily sync between devices, OS's, etc.

- Other benefits depending on password manager

Password Policy Practical Implementation



For more detail: <https://info.knowbe4.com/wp-password-policy-should-be>

Agenda

- Why Use a Password Manager?
- Common Features of a Password Manager
- How Password Managers Can Be Attacked
- How to Best Defend Your Password Manager

Common Features of a Password Manager?

- There are dozens of password managers
 - Free, open source, and commercial
 - Many vendors have free and commercial versions
 - Part of browser, part of an OS, part of a security suite, or stand-alone
 - Most only support some OS's and browsers (you need to check)
 - Desktop clients and/or browser extensions
 - Only some have enterprise support, if you need it
 - Some have family plans
-
- <https://www.wired.com/story/best-password-managers/>

Common Features of a Password Manager?

Some Popular Stand-Alone Password Manager Vendors

- 1Password (1password.com)
- LastPass (lastpass.com)
- KeePass Password Safe (<https://keepass.info/>)
- Password Safe (<https://pwsafe.org/>)
- Bitwarden (bitwarden.com)
- KeePass (keepass.com)
- Keeper (keepersecurity.com)
- oneSafe (onesafe-apps.com)
- Enpass (enpass.io)
- Roboform (roboform.com)
- Norton
(my.norton.com/extspa/passwordmanager)
- AuthPass (authpass.app)
- Dashlane (dashlane.com)
- Nordpass (nordpass.com)

Common Features of a Password Manager?

Some password manager review articles

- <https://www.wired.com/story/best-password-managers/>
- <https://www.nytimes.com/wirecutter/reviews/best-password-managers/>
- <https://buyersguide.org/password-manager/t/best>
- <https://www.top10cybersecurity.com/password-manager>

Common Features of a Password Manager?

- Stand-alone password managers are usually better:
 - Company's entire focus
 - Better feature sets
 - More frequently updated
 - Not usually tied to a single OS or browser

- <https://www.wired.com/story/best-password-managers/>



Common Features of a Password Manager?

Some Features Beyond Just Storing Password

















- Create perfectly random passwords (must-have)
- Auto-filling (must-have in my opinion)
- Password strength review (including comparing to other existing passwords)
- Automatic notification of breached passwords
- Can use MFA to protect password manager instead of master password
- Password manager can simulate some MFA types for user logon
- Clipboard auto-expiration
- Secure notes and safe online storage of other documents

Common Features of a Password Manager?

Some Features Beyond Just Storing Password

- **Vulnerable Password**
This password appears on a list of exposed passwords. Change your password. [Learn more about the haveibeenpwned.com service.](#)
-  Citi
- ro****12
- Terrible 
- <https://online.citi.com/US/login.do>

Additional features shown in a grid:

 Login +	 Secure Note +
 Credit Card +	 Identity +
 Password +	 Document +
 API Credential +	 Bank Account +
 Crypto Wallet +	 Database +
 Driver License +	 Email Account +
 Medical Record +	 Membership +
 Outdoor License +	 Passport +

Additional text on the right side of the slide: "ords", "nior", "ding", "ed p", "d n", "e so", "ords)"

Common Features of a Password Manager?

How to Pick a Password Manager

- Read some reviews
- Inventory what OS's, devices, and browsers you must have support on
- Do you want automated device sync?
- Do you mind paying an annual fee?
- Do you need enterprise support?
- Pick a few to try yourself
- Pick a long-lasting vendor which cares about security

Common Features of a Password Manager?

Where Are Your Passwords Stored?

Very important to risk consideration

- Locally only
- File-based
- Portable devices
- Sync'd across devices
- With vendor
- In the cloud

Agenda

- Why Use a Password Manager?
- Common Features of a Password Manager
- How Password Managers Can Be Attacked
- How to Best Defend Your Password Manager

Password Manager Attacks

- As great as password managers are, they do represent a single-point-of-failure risk
- What if hacker accesses all your passwords all at once?

- This is a real risk!

Password Manager Attacks

General Types

- Remote attacks
- Local attacks
- Vendor attacks

Password Manager Attacks

Remote Attacks

- Attacker is not on victim's desktop to start with, but is targeting victim

Password Manager Attacks

Remote Attacks

- Most common remote attack is social engineering
- Get victim to reveal password to fake website
- Usually will not work if victim uses password manager's auto-logon or auto-fill-in feature (if password manager has it)
- What often happens is the victim gets frustrated thinking the password manager is not working for some unknown reason and doesn't realize it is a phishing attack with a bogus URL, and they manually copy/paste the password
- Must train yourself to be on the lookout for these types of attacks!
- Force yourself only to use auto-logon or auto-fill-in feature and to be suspicious and investigate if they don't work as expected

Your subscription is about to expire.



Netflix <admin@mofity.com>

To Roger Grimes

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



Your subscription is about to expire.

[Update Profile](#)

Unfortunately, we were unable to renew your subscription.

If you choose to keep your subscription active, you must update your profile.

<http://www.ilianniguitars.com/730248246046084758023602483829234958152431374385989587435130472122678806082437363274059846790>

Click or tap to follow link.

Password Manager Attacks

Other Remote Attacks

- Get victim to download trojan horse program
- Remote attack – unpatched vuln or misconfiguration

Attackers have started using the Citadel Trojan program to steal master passwords for password management applications and other authentication programs.

The malware, called Masslogger, is a Trojan horse that arrives as an email attachment. It tries to steal usernames and passwords from Microsoft Outlook, the Thunderbird email client, NordVPN, Discord and other email and chat services, as well as from the password managers built into Google Chrome, Mozilla Firefox, Microsoft Edge and other browsers.

RedLine malware shows why passwords shouldn't be saved in browsers

Even though the infected computer had an anti-malware solution installed, it failed to detect and remove RedLine Stealer.

The malware targets the 'Login Data' file found on all Chromium-based web browsers and is an SQLite database where usernames and passwords are saved.

Password Manager Attacks

Other Remote Attacks

- Get victim to download trojan horse program
- Remote attack – unpatched vuln or misconfiguration
- Essentially game over
- Although if your password manager is not open, attacker often can't immediately access all the passwords
- Attacker can wait for user to logon, install keylogging trojan, or try some other trick

Password Manager Attacks

Local Attacks

- Hacker is on victim's desktop
- Essentially game over
- Although if your password manager is not open, attacker often can't immediately access all the passwords
- Attacker can wait for user to logon, install keylogging trojan, or try some other trick

Password Manager Attack Video

Attack Demo

- By KnowBe4's Chief Hacking Officer, Kevin Mitnick
- Attack assumes hacker is already on network with victim's IP address and password, just trying to access passwords on victim's locked password manager remotely
- 4:02min long

```
Hostname : DESKTOP-I5M37ER
Instance ID : i-034891567e44e3889
Public IP Address : 3.106.80.120
Private IP Address : 172.31.29.228
Availability Zone : ap-southeast-2c
Instance Size : t2.medium
Architecture : AMD64
```

Recycle Bin



Bitvise SSH Client



Google Chrome



KeePass 2



clean-start.bat
at



Type here to search



5:11 AM
4/13/2022



Password Manager Attacks

Vendor Attacks

- Password manager vendors are attacked
- Password manager employees are socially engineered
- Password manager programs contain bugs
- Password manager vendor's network resources can be hacked

Vulnerability Trends

Year	# of Vulnerabilities
2018	1
2019	1
2020	4
Total	6

Massive LastPass Hack Affects 30 Million Users. Is Your Data at Risk?

Year	# of Vulnerabilities
2012	1
2018	1
2020	2
2021	4
2022	2
Total	10

Password Manager Attacks

Vendor Attacks

- But anything can be hacked
- The software you use the most (e.g., operating system, browser, email, etc.) is hacked all the time and you still use it
- “Bad” password manager attacks have happened...and most users are still using the programs and doing fine
- Worst case scenario once you find out about compromise is you have to quickly change all your stored passwords (and of course, any resulting damage before you were able to change your passwords)

- Does password manager vendor patch bugs quickly?
- Does password manager vendor seem to care about security?

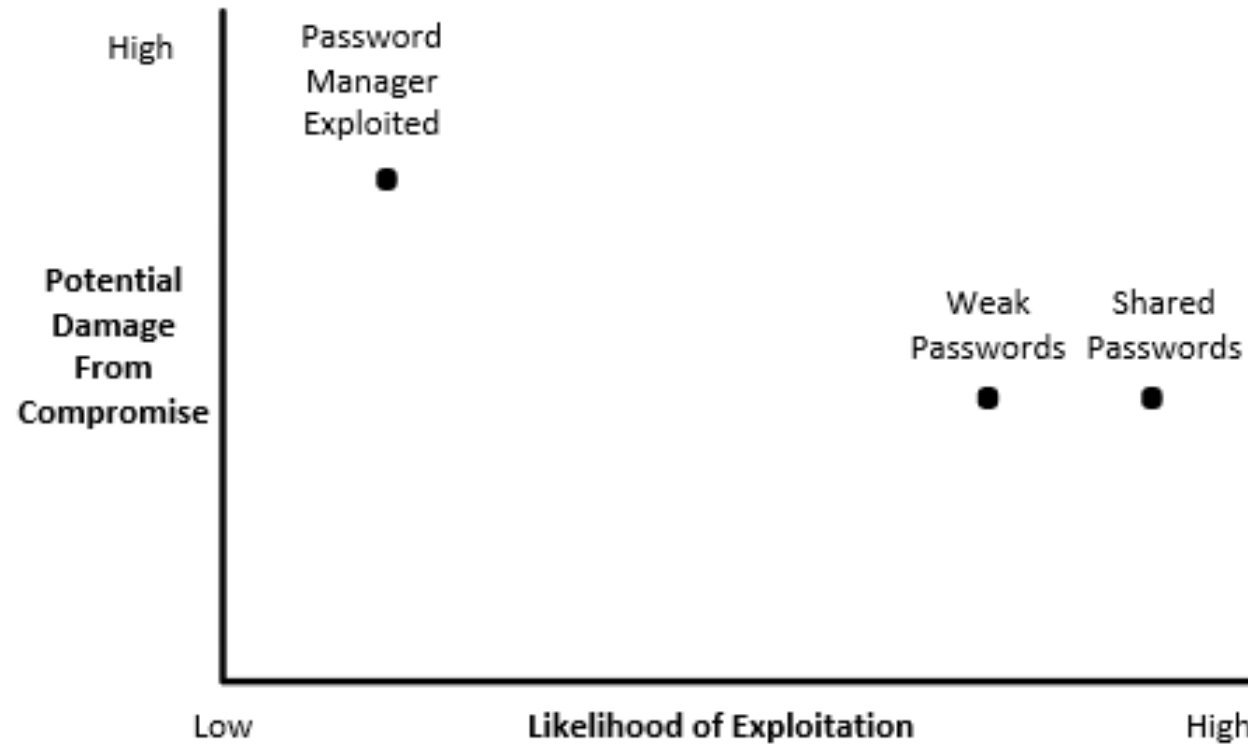
Password Manager Attacks

Ultimate Password Manager Risk Decision

- Password managers reduce the HUGE risk of you using the same password (or pattern) across multiple, unrelated sites and using weak passwords
- Mitigating these two risks likely outweighs the single-point-of-failure risks

Password Manager Attacks

Ultimate Password Manager Risk Decision



Password Manager Attacks

Ultimate Password Manager Risk Decision

- Password managers reduce the HUGE risk of you using the same password (or pattern) across multiple, unrelated sites and using weak passwords
- Mitigating these two risks likely outweighs the single-point-of-failure risk

And also consider...

- Password managers prevent social engineering of your passwords!
 - Which is a HUGE risk!
- If hacker is on your local desktop, which is most of the risk, it's game over anyway, with or without a password manager involved
- Yes, you must consider new risk of vendor compromise
- You'll have to decide whether it's worth the risk or not

Agenda

- Why Use a Password Manager?
- Common Features of a Password Manager
- How Password Managers Can Be Attacked
- How to Best Defend Your Password Manager

Picking a Good Password Manager

Does Vendor Really Care About Security?

- Security Development Lifecycle (SDL) programming
- Strong, Industry-Accepted Encryption (don't "roll their own")
- Has strong defaults
- Has strong security features, like MFA
- Is transparent in what they do
- Is responsive to bug reports
- Is responsive to community
- Participates in bug bounties
- Can you trust vendor to protect your passwords?

Defending Your Password Manager

- Pick a good password manager and password manager vendor
- Watch out for social engineering attacks!
- Use phishing-resistant MFA if you can to protect your password manager
- Use phishing-resistant MFA or passkeys to protect your valuable data and programs, if allowed
 - For info on passkeys: <https://www.linkedin.com/pulse/youll-likely-using-passkey-soon-roger-grimes/>
- Use a long master password (20-char or longer if made up by you)
- Let password manager create your perfectly random passwords, at least 12-characters long, for your sites and services (use auto-logon/auto-fill features)
- Change your passwords at least once a year
- Set password manager lock time-out to some non-long interval, just don't leave open all day or forever (give yourself a chance not to be hacked)

Defending Your Password Manager

- Don't be socially engineered
- Get good, aggressive security awareness training
- Patch your desktops/devices in a timely manner
- Look for and resolve configuration mistakes



Breached Password Test

» [Check Your Passwords](#)

KnowBe4's free **NEW Breached Password Test (BPT)** checks to see if your users are currently using passwords that are in publicly available breaches associated with your domain. BPT checks against your Active Directory and reports compromised passwords in use right now so that you can take action immediately!

Here's how Breached Password Test works:

- ✓ Checks to see if your company domains have been part of a data breach that included passwords
- ✓ Checks to see if any of those breached passwords are currently in use in your Active Directory
- ✓ Does not show/report on the actual passwords of accounts

- <https://www.knowbe4.com/breached-password-test>

KnowBe4 Security Awareness Training



Baseline Testing

We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.



Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.



Phish Your Users

Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.



See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

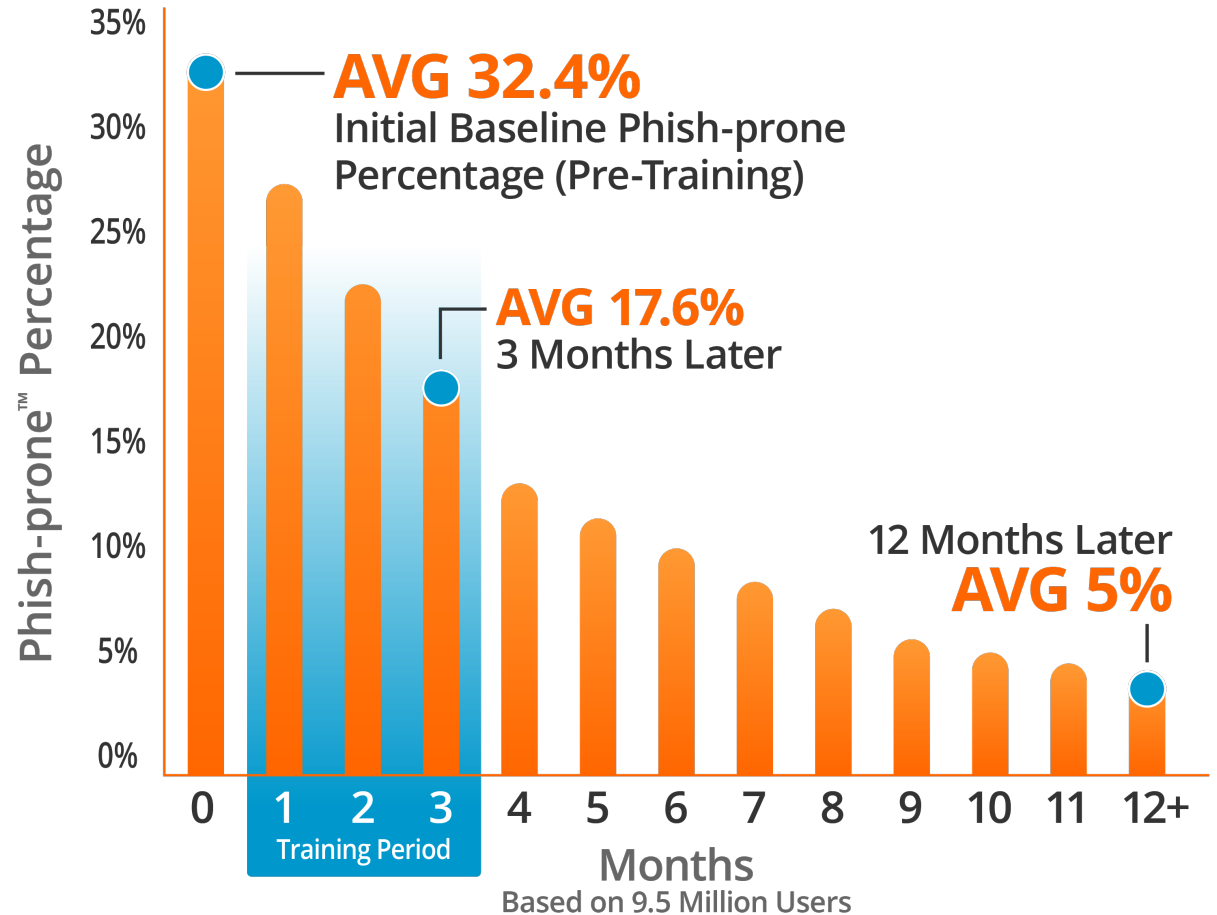


Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

85% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

Roger A. Grimes— Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)

<https://www.linkedin.com/in/rogeragrimes/>