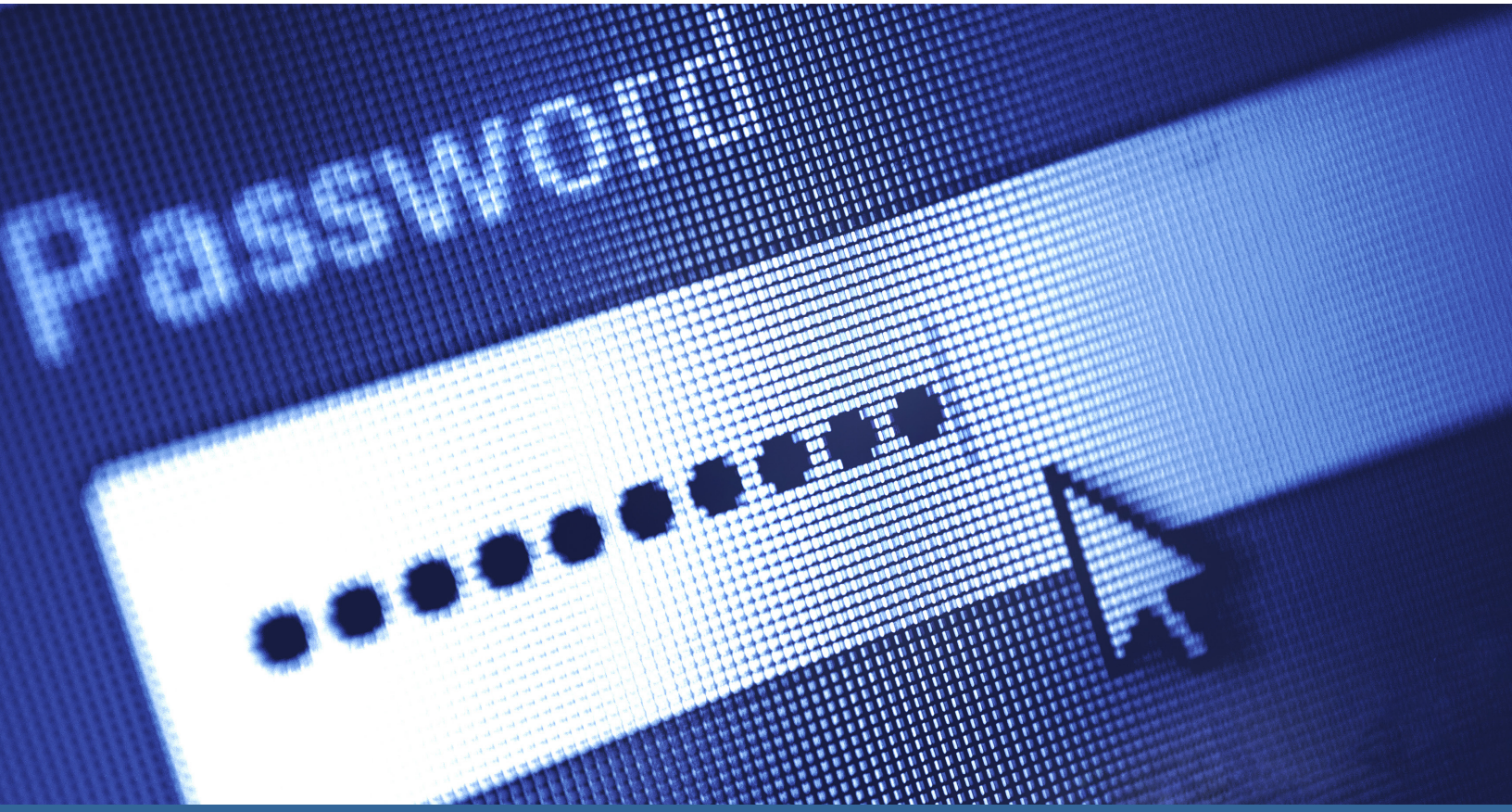
KEVIN MITNICK
Security Awareness Training



Strong Passwords

Passwords

Always use strong passwords on the Internet. A strong password is one that is hard for someone else to guess.

Kevin Mitnick's 10 Rules for Stronger Passwords

- ☐ Don't tell your passwords to anyone! Nobody should ask for your passwords, and you should never give your passwords to anyone. Normally, tech support does not need your password to get into your account, so there's no reason for a legitimate tech support person to ever ask for your password.
- ☐ Don't use simple dictionary words, pets' names, or people's names for passwords. Avoid easy-to-guess numbers, such as your age, zip code, birthday, or anniversary.
- ☐ Use passwords that are at least 20 characters long. And do not write them down where they can be easily found.
- ☐ Create a "pass phrase" instead of just one word (for example, $3 for the pirate hat). Or think up a few nonsense words that you can remember easily (for example, Betty was smoking tires and playing tuna fish).
- ☐ Use a different password for each website. Do not use simple patterns like "password1""password2", "password3" or "amazon4me", "netflix4me", "yahoo4me" for different sites – those are too easy to guess.
- ☐ Change your passwords for sensitive web sites (such as your online banking) every 60-90 days. Do not use easy-to-guess patterns when you change them.
- ☐ If you think someone may have learned your password, change it immediately. Then check the websites where you use that password for any signs of misuse – starting with your online banking site.
- ☐ Sometimes websites ask you to enter the answer for a "security question" you can use if you forget your password. Make your answer to the security question just as hard to guess as your password.
- ☐ If your bank or webmail offers you extra security features, use them!
- ☐ Use the password procedures your company requires, and at home consider using a password manager such as KeePass or Password Safe. Password managers make your Internet use a lot safer and easier.

"It's important to keep malware (malicious software) off your computer so hackers cannot intercept your passwords. Even if your passwords are very strong and hard-to-guess, malware can still allow a hacker to get them."

- Kevin Mitnick

"You can safely give out personal information if YOU contact an organization that you have some business with, and they have a legitimate need to ask for that information.

"But always suspect a problem if THEY contact YOU in a way you cannot verify."

- Kevin Mitnick

Giving Out Personal Information

Criminals can use your personal information to harm you – to steal your money, steal your identity, and ruin your reputation and your credit.

Even if someone tells you they are from your bank or your credit card company, you should never reveal this kind of information to anyone unless you started the contact, and you know you are talking to a legitimate organization.

Stop – Look– Think before you give out personal information

- ☐ Be careful when you get an automated phone call with a recording that asks you to verify your identity, your credit card number or other personal information. Do not provide that information!
- ☐ Do not trust any telephone numbers you are sent in an email. Use Google to look up the real phone number you need to call, then you call them.
- ☐ Don't ever give out your Social Security number unless there is a legal requirement to do so.
- ☐ Don't respond to anyone asking for personal information through social media like Facebook, email, text or phone for information like your Social Security number, bank account number, date of birth, address, or driver's license number unless you initiated the contact to a number or website you can verify.
- ☐ Consider using an identity theft notification service that alerts you if your (or your children's) personal information is posted on the Internet.

What is "Personal Information"?

Personal information is defined as: First name (or first initial) AND last name AND at least one of these items:

- Social Security #
- Driver license or state-issued ID #
- Military ID #
- Passport #
- Credit card (or debit card) #, security code, and expiration date
- Financial account #s (with or without access codes or passwords)
- Customer account #s
- Unlisted telephone #s
- Date or place of birth
- Mother's maiden name
- PINs or passwords
- Password challenge question responses
- Account balances or histories
- Wage and salary information
- Tax filing status
- Biometric data that can be used to identify an individual, (e.g., finger or voice prints)
- Digital or physical copies of handwritten signature
- Email addresses
- Medical record #s
- Vehicle identifiers and serial #s, including license plate #s
- Medical histories
- National or ethnic origin
- Religious affiliation(s)
- Physical characteristics (height, weight, hair/eye color, etc.)
- Insurance policy #s
- Credit or payment history data
- Full face photographic images
- Certificate/license #s
- Internet Protocol (IP) address #s

About KnowBe4

KnowBe4 is the world's most popular integrated Security Awareness Training and Simulated Phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created by two of the best known names in cybersecurity, Kevin Mitnick (the World's Most Famous Hacker) and Inc. 500 alum serial security entrepreneur Stu Sjouwerman, to help organizations manage the problem of social engineering tactics through new school security awareness training.

More than 1,700 organizations use KnowBe4's platform to keep employees on their toes with security top of mind. KnowBe4 is used across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance.

- KnowBe4 wrote the book on cyber security (8 books and counting between Mitnick and Sjouwerman).
- KnowBe4 is the only set-it-and-forget-it security awareness training platform "by admins for admins" with minimum time spent by IT to get and keep it up and running.
- The platform includes a large library of known-to-work phishing templates.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, LLC | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com