ALAMO COLLEGES DISTRICT

Northeast Lakeview College • Northwest Vista College
Palo Alto College • St.Philip's College • San Antonio College

SECURITY Smart™

NEWSLETTER FALL 2017

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Inside 4 Common Password Myths

WHETHER YOU'RE ON email or social media, online banking or gaming, any site that stores your data still depends on strong passwords to keep miscreants out.

By now, most people know the basics—don't use "password," and don't repeat the same password across different accounts. But a lot of standard password advice really needs some additional context to be helpful. Here are some ubiquitous password myths, clarified.

Myth 1: Passwords need to have mixed cases, numbers and special characters.
Truth: Yes, but that's not enough to guarantee maximum security. For example, "letmein" is no good, but "Passw0rD" isn't really any better. Creating passwords based on dictionary words is a bad idea, and even substituting some of the letters for numbers or symbols isn't helpful. Password crackers know to include words like "vuln3rabl3" or "trustno1" in their lookup tables.

To be fair, using mixed cases, numbers and special characters does make a password much stronger than lowercase letters alone. Consider that a computer might take two days to crack an eight-character password that is all lowercase, but a large botnet will take only 1.8 seconds. Mixing cases helps slow down the cracking, and throwing in a special symbol or two bumps up the number of combinations.

But all the mixed cases, numbers and special characters won't do any good if the string isn't actually random, as in "1q2w3e4r." Password crackers can look at the keyboard to find potential patterns, too.

Myth 2: A good password must be extremely long.
Truth: Longer is definitely better, but 10 to 12 characters can be adequate. Shorter passwords take far less time to crack. On a strong botnet, an eight-character password that uses mixed cases and numbers will take just 31 minutes to figure out; increasing the password to 10 characters will take that same botnet 83 days.

If the concern is that someone will break into a database and steal passwords, then extremely long and complex passwords are definitely the way to go. But usually the issue is password reuse and phishing, and if attackers have already intercepted the actual password, it doesn't matter if it's eight characters or 50. They just copy and paste, and they're in.

Myth 3: Never write down passwords.
Truth: The issue is more about where you keep it once written. Don't jot down "My new 401K password for Fidelity" on a sticky note and put it on your desk, cautions Chet Wisniewski, a security expert with antivirus company Sophos, "but writing down a new, long, complex password while you burn it into your memory and keeping it in your wallet or purse for a week until you get that muscle memory of typing it isn't really a problem." He also writes down important passwords and stores them in a safe deposit box so that his family can "unlock our lives" in case of an emergency.

Myth 4: Periodically changing passwords improves security.
Truth: This strategy might just make it more likely that you'll select weak passwords you find easier to remember. Frequent password changes make sense if the primary concern is that passwords might be leaked or exposed, and if there is proof that your passwords were exposed, a password reset is a good idea. But changing passwords just because an arbitrary number of days have passed? Not really necessary.

IRS Scams 2017: What You Need to Know Now

IRS scams are so widespread that they've affected how the agency works, delaying legitimate refunds to many taxpayers. Here's a look at some of the different types to watch out for.

- **Phone calls to individuals** telling them they owe back taxes and threatening arrest if payment isn't immediately received.

How to protect yourself: Hang up the phone. The IRS does not call taxpayers out of the blue and will never threaten you with arrest. Your mailing address and employment history may be easy to find online, so even if someone on the phone has that information, that doesn't necessarily mean they're from the government.

- **Phishing emails sent to individuals** that request PINs, passwords and bank account information, ostensibly to allow the IRS to send a big refund. Instead, scammers use the information to drain the victim's account.

How to protect yourself: The IRS will never request this kind of information via an unsolicited email. If you are confused by the nature of an email you receive, don't reply to it; instead, contact the IRS directly. Never send financial information of any kind in response to an unsolicited email. Report unsolicited email claiming to be from the IRS to **phishing@irs.gov.**

- **Phishing emails sent to payroll or HR**, looking to get taxpayer ID information that can be used to file fraudulent returns or other documents. The attacker might masquerade as an executive in the personnel or human resources division of the company and email a lower-level worker in those departments requesting copies of employee W-2 forms.

How to protect yourself: You need help with this one. Make sure your employer's IT or security department and anyone who has access to employee records are aware of this scam. Never share your W-2 with anyone but your tax preparer.

- **Scam letters sent via "snail mail."** If the IRS does want to initiate contact with you, it will generally do so the old-fashioned way: by sending you a letter in the mail. Scammers can try to create fake versions of these as well.

How to protect yourself: A real letter from the IRS will include a notice code explaining exactly what the topic of the letter is. For more information about the codes, go to **www.irs.gov** or call the tax help line for individuals at 1-800-829-1040.

7 Signs an Email Is Bad News

BACK AWAY FROM an incoming email if you spot any of these issues, and alert your IT department right away.

1 Links in the email that have a questionable domain name. (Do not click on links in unsolicited email!)

2 Typos or grammatical mistakes, or a weird-sounding subject line.

3 Your name is not in the To: or CC: line, or many of your colleagues or friends are listed as recipients.

4 The email appears to be from an internal address at your company but contains some suspicious details. If this happens, do not reply to the possibly fraudulent email, as phishers can easily spoof an address so it looks like it's from a trusted source. Instead, test its validity by creating and sending a new, unique message to the address of the alleged sender.

5 A request for sensitive information, like your address, bank account numbers, Social Security number, or date of birth. No legitimate company will try to collect this information from you blindly, especially via email.

6 A password change request. If an email asks that you change one of your account passwords by clicking on a link, don't do it. Even if the email seems legit, open a browser and type in the proper URL for the site in question instead. Then if it's really needed, you can change your password after you log in to your account.

7 "Big bucks in your future!" Sadly, any email that claims that money has been left in your name or says you have won money is fake. Ditto for any email asking you to send money.

DID YOU KNOW?

57.6 days: The average time it took to detect a security breach in 2015.

92.2 days: The average time it takes in 2017. This means hackers now have an extra month to roam around corporate systems, gathering data, stealing money, sapping bandwidth, and changing code.

SOURCE: 2017 U.S. STATE OF CYBERCRIME SURVEY

Should You Buy a Kid-Tracking Smartwatch?

A new report found security flaws in smartwatches designed for children.

SMARTWATCHES FOR KIDS are marketed as a way for parents to remotely keep tabs on their offspring, but a recent report claims the devices have serious privacy and security flaws that could allow a stranger to seize control of the watches and use them to track and eavesdrop on children.

The Norwegian Consumer Council (NCC) and the security firm Mnemonic tested four smartwatches for kids that included features such as location tracking, microphones and cameras for remote monitoring of children by parents. The watches were all available in both physical Norwegian retail stores and online, and were also marketed under different brand names in other countries. Mnemonic discovered "significant security flaws in three of the four devices tested, which may lead to information about GPS watch users' location and activities ending up in the wrong hands. The flaws are not technically difficult to exploit, and in two cases, allow a third party to covertly take control over the watch."

"It's very serious when products that claim to make children safer instead put them at risk because of poor security and features that do not work properly," said Finn Myrstad, director of digital policy at the NCC. "Importers and retailers must know what they stock and sell. These watches have no place on a shop's shelf, let alone on a child's wrist." And, as NCC's report added, "the vast variety of products being imported and sold under different names also make it exceedingly difficult to understand who is responsible for any problems with the devices or apps."

Some of the smartwatches for kids are being sold in the United States. Seven consumer watchdog groups are now asking the FTC to look into the risks to children's safety associated with the devices and to determine if they violate laws such as the Children's Online Privacy Protection Rule. (The advocacy coalition is the same one that called on the FTC to take action against "toys that spy.")

The coalition explained to the FTC that two of the devices allow potential attackers to take control of the apps, giving them access to kids' current and past location and personal details, and possibly allowing them to contact kids directly—all without the parents' knowledge. In addition, key features, including an SOS button for the wearer to push in the event of emergency, were unreliable.

The data privacy practices of the firms also place children at risk, the group said. One company allows children's personal data to be used for marketing purposes, while another transmits unencrypted location data. Only one of the companies asks for consent prior to data collection.

SECURITY THREATS: WHAT WE FEAR MOST

What are the top security threats people think they face as individuals? Here's what respondents in a recent survey about cybersecurity said:

1. Identity theft
2. Stolen credit cards and fraudulent charges
3. Spam and phishing emails
4. The physical security of home and property
5. Accessing and draining of bank accounts

SOURCE: BLUMBERG CAPITAL SURVEY

6 Tips for Road Warriors

WHEN YOU TRAVEL for work, you could be a prime target for hackers. Take these steps to keep your devices—and the data they contain—safe.

Safeguard your mobile devices. All devices should be equipped with technology such as password protection, encryption, data backup and remote data wipe capabilities, in the event that they go missing. In the airport, don't push your laptop through the X-ray until you are ready to proceed yourself. Don't leave it at your table in Starbucks while you fetch your latte. Someone can grab it and go in an instant.

Stick to password-protected Wi-Fi. Use a secure communication channel or secure corporate virtual private network for all network connections.

Be aware of your surroundings. Situational awareness is key. Who are you talking to? Who knows where you're going? Sharing information with the wrong parties can make you an easy target.

Look out for shoulder surfers. Make sure no one can peek at your confidential information on upcoming presentations, business pitches, stock purchase movements and the like simply by glancing over at you while you're on a plane or train, or sitting in a coffee shop.

Inform your company's security/IT department of your specific travel plans. Check your organization's policies regarding security precautions for travel generally and for your destination. If possible, provide an itinerary. That way, an attempt to access your employer's network from, say, London when you were scheduled to leave there two days ago will ring security's alarm bells.

Time to Discard Your Old Device? Wipe It First!

Though people usually attempt to wipe, or delete, their personal information from older electronic devices before getting rid of them, a recent study found that many show up on the secondhand market containing the previous owner's personally identifiable information (PII), from credit card numbers to company data.

The National Association for Information Destruction (NAID), a trade association, recently bought a slew of secondhand smartphones, tablets and hard drives for the study; 40 percent of them contained PII that NAID was able to retrieve and transfer using commercially available technology from CPR Tools.

"As data storage is included in nearly every aspect of technology today, so is the likelihood of unauthorized or unintended access to that data," said CPR Tools CEO John Benkert. "Auction, resell and recycling sites have created a convenient revenue stream in used devices; however, the real value is in the data that the public unintentionally leaves behind."

According to NAID, recycled IT equipment is supposed to go to a qualified service provider specializing in secure data destruction, and obtain legally binding assurance that the recycler is accepting that responsibility. Too often, though, the organization claims to be erasing the data, but the contractual fine print (or terms and conditions) disavows any legal responsibility, instead stating it is the responsibility of the individual to remove the data first.

PII recovered included company and personal data, credit card information, contact information, usernames and passwords, tax details, emails and more. The tablets were the devices most likely to contain recoverable PII, at 50 percent, compared with 44 percent of hard drives and 13 percent of mobile phones.

Robert Johnson, NAID CEO, cautions that the results are not an indictment of reputable commercial services providing secure data erasure. "We know by the ongoing audits we conduct of NAID Certified service providers that when overwriting is properly done, it is a trustworthy and effective process," he said. "The problem lies with service providers who are not qualified and, too often, with businesses and individuals who feel they can do it themselves."

4 Easy Ways to Lose Your Valuable Company Data

Losing data can be expensive: A recent IBM study found that the cost associated with each lost or stolen record containing sensitive and confidential information is $158. And data exposure can ruin an organization's reputation. David Zimmerman, CEO and founder of data recovery firm LC Technology, lists four ways individuals might cause companies to lose data—and how to avoid them.

Changing advanced settings

The "advanced settings" feature on computers is not there just for show. It's a serious warning to users that they had better know what they are doing before they start making system changes. A frequent example of that kind of setting involves the BIOS (basic input/output system), the chip that instructs the computer what steps to take after the power is turned on. Changes to this setting can be made with the best intentions, but they might expose the machine to data loss or theft. Advanced settings adjustments are best handled by IT.

Being exposed to ransomware

Ransomware is a hacking scheme that involves taking over a person's computer files, encrypting them and then asking for a ransom to pay for the encryption key. Hackers typically gain access through email attachments or by guessing passwords. Data loss comes when the hackers steal valuable information during the ransom period, or if the ransom isn't paid, the hackers will typically leave the data encrypted or destroy it beyond repair. To avoid being attacked, never click on unexpected or suspicious-looking email attachments, and use complex passwords. (For more about passwords, see page 1.)

Not following security protocols

Many of the hacking incidents reported in the news are caused by simple human error. Learn and follow your employer's security guidelines, for physical spaces as well as virtual ones.

Using improper backup procedures

A very common reason for data loss (especially among smaller companies) is if data is stored locally and not backed up, and a system fails or is damaged or compromised. Businesses should have strict backup procedures for their corporate data, including processes for individual employees and departments—ask your IT department if you're not sure what the protocol is.

CSO FROM IDG

Security Smart is published by CSO, the leader in news, analysis and research on security and risk management. © 2017 IDG
To purchase an individual subscription, email **securitysmart@csoonline.com** or **marketing@idgenterprise.com** for more information.

About the Enterprise IT Risk and Security Office

Overview

The District Enterprise IT Risk Management and Security Office supports the Alamo Colleges' mission by providing IT risk management services and information security safeguards to help reduce IT risks, enhance security posture, facilitate compliance and improve on continuous operation efficiency and effectiveness.

Mission Statement

The Enterprise IT Risk and Security Office will strive to succeed its mission by acquiring, developing, implementing, measuring and maintaining cost effective and efficient safeguards which support the confidentiality, integrity, availability, and compliance requirements of information technology-based resources and services for Alamo Colleges.

Meet the Staff

Oscar T. Salazar CISSP, CISA, GIAC, GSNA
District Enterprise ITS Risk and Security Manager
210-485-0403
osalazar25@alamo.edu

Tommie Banks CCNA, CCNA-SECURITY, CEH
District Enterprise ITS Risk and Security Analyst
210-485-0478
tbanks22@almao.edu

Helpful Links

Enterprise IT Risk and Security Office Website
http://share.alamo.edu/securityawareness/default.aspx

Reporting Phishing Incidents
Phishing_Abuse@alamo.edu

Did you know?

A Banner workflow is being developed to automate the Banner Request process… Stay tuned more to come.