April 2017

SecurityAwarenessNews

the security awareness newsletter for security aware people

Top 10 Security Practices for Work, Home & On the Go!

Plus More!

10 STATS to PONDER

Statistics are important. While they can be presented in many ways independent of context to push an agenda, the numbers don't lie when it comes to privacy and the protection of sensitive data. We use them, not in an attempt to push a false sense of fear, uncertainty, or doubt, but as a way of showing just how big the global cybercrime industry is.

Knowledge is power. And, in this case, that power enables us to protect ourselves, our organizations, our families, and our friends. Check out these ten statistics and consider how each one could affect you. Remember that each and every one of us has it in ourselves to be a strong human firewall and combat cybercrime!

10

According to the 2017 Annual Threat Report conducted by SonicWall, ransomware attacks increased from **3.8 million** in 2015 to **638 million** in 2016.

9

2016 set an **all-time high** in data breaches, with over **4 billion** records exposed globally.

8

The price of **bitcoin** is nearing the highest in its existence, which means the price for **ransomware** is likely going to climb.

7

Over **70%** of organizations report having been compromised by a cyber-attack **in the last 12 months**.

6

63% of confirmed data breaches leverage a **weak, default, or stolen password**.

5

Cybercrime is expected to cost **$6 trillion (€5.7 trillion)** globally **by 2021**.

4

Four out of **five** victims don't realize they've been attacked for a **week or longer**.

3

Over 30% of phishing emails **are opened**.

2

Cybercriminals take only **minutes** (or less) to compromise systems in **93% of breaches**.

1

7% of data breaches go **undiscovered** for more than a **year**.

SOURCES:

(10) https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/
(9) https://www.riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records/
(8) http://www.coindesk.com/bitcoin-rebounds-two-month-low-top-1000/
(7) http://www.securityinfowatch.com/news/12208393/study-nearly-three-quarters-of-organizations-have-suffered-a-cyber-attack
(5) http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
(4 & 6) http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
(1, 2 & 3) https://www.bitsighttech.com/blog/data-breach-statistics

Good security comes from timely response. Report security incidents immediately!

TOP 10 WAYS TO STAY SAFE AT HOME

Update default passwords for all internet connected devices immediately. This includes routers, smart TVs, game consoles, and anything that requires a login.

Every device and every account needs a strong and unique password. Or, even better, a passphrase!

The admin account is for one person: **you**. Don't give those credentials to other members of your household.

When setting up your wireless router, be sure to use the proper encryption, such as WPA2. Older versions, like WEP, are no longer secure.

Enable automatic updating for software and firmware. You'll want all of your devices on the latest and greatest so as not to miss out on important security patches.

Disconnect any devices that are no longer being used or whose internet connection is rarely used.

Physically protect your devices! Use surge protectors, power things off during strong thunderstorms, and be careful with liquids near any technology.

Back it up! Your phones, your laptops, your tablets all store data that you probably want to keep. Back those devices up both locally and remotely.

Create a family security policy. Develop a set of rules for you and everyone in your household to follow. Remember that policy violations should come with consequences!

Use internet monitoring software to know what your kids are doing online. And explain to them why it's important!

How do you protect your kids from online threats?

Children of all ages are major targets for cybercriminals (and cyberbullying). Protecting them online is an especially difficult task these days considering how many avenues they have to connect. But we have a combination of tools and real-life lessons at our disposal to assist us. It starts with knowing what we're up against (identifying the threats). Then, we can leverage the tools and technologies designed to mitigate those threats. Did you know, almost 10% of kids aged 18 and under have had their identity stolen and most don't even know? Know their credit scores and consider an ID Protection monitoring service for them, too. Eventually we'll change long-term behavior and raise smart and safe digital citizens. **Learn more: secaware.co/2jlaLFc.**

Good security comes from timely response. Report security incidents immediately!

Top 10 Security Practices *For Work*

- Report anything unusual. Whether it be a suspicious package or someone who doesn't belong, if you see or hear something, say something!
- Think before you click. CEO scams—social engineering attacks that spoof the email of an executive—are on the rise.
- Trust but verify. If you do receive an email requesting financial transactions or sensitive information, verify that it's legit. Sometimes a quick phone call is all it takes.
- Use strong, unique passwords for every account! In fact, use passphrases with symbols, numbers, and letters for added security. Turn on two-factor authentication wherever possible.
- Keep it clean. A messy desk is a security risk. Keep your work area clean and organized.
- Be aware of unsolicited hardware. Never plug in random USB drives or optical discs. Even a keyboard or mouse can be a security threat! (Read more: secaware.co/2lp5Rki)
- Be aware of the kind of data you handle. Understanding data classification is essential for knowing what needs to be protected!
- Only use approved devices. We put a lot of effort in maintaining a safe and secure network. Be sure to ask before connecting with a personal device at work.
- Know how to properly dispose of sensitive info. Shred sensitive documents. Ask about disposing of old computers or devices.
- Always follow policy. Policies are in place for the benefit of everyone within the organization. If you're not sure, please ask!

– WHY IS – *data classification* so important?

A better question to ask is, "**How can you protect information unless you know what exactly you are trying to protect?**" Data classification is a way of categorizing sensitive information so you can be familiar with where it exists, how it needs to be protected, and why it needs to be protected. Read more: secaware.co/2lp5Rki.

What is CEO Fraud?

Also known as a Business Email Compromise (BEC), a CEO fraud is an exponentially growing scam by which the attacker spoofs the email address of a high-level executive and emails requests for information or financial transactions to other employees. Over the last three years **this scam has cost organizations billions globally**, and attacks are expected to increase this year. So, it's imperative that we **always confirm the source of an email**, be on the lookout for anything that seems odd or off, and, if you even have so much as a shadow of a doubt, report it! Trust your instincts and use common sense!

Good security comes from timely response. Report security incidents immediately!

Top 10 Ways To Stay Secure On The Go

Between our lives at work and home exists an attack surface known as mobile. Our phones, tablets, and laptops easily outnumber people in the world, and cybercriminals have taken note. These connected devices have provided the bad guys a way to target us no matter where we are or what we're doing. As a result, we need to take extra precautions when connected on the go!

1. **Install anti-virus and anti-malware software on all devices. Computers aren't the only ones at risk of infections.**
2. **Never connect to public networks without a VPN. VPNs (virtual private networks) encrypt your connection and protect your information.**
3. **Put a sticker on it! Theft of devices is a major concern at airports, coffee shops, etc. Deter thieves by personalizing your laptop/devices with stickers or unique cases.**
4. **Enable remote access. Both Android and iOS have built in features that allow you to connect remotely to your device, change the password, ping it to ring, and completely reset it in the event of loss or theft.** (Read more: secaware.co/2icj6Uu)
5. **Lock it up. All of your devices need to be protected with a strong, unique password of some sort (a pin or a pattern, for example). But be careful with biometrics, like fingerprint scanners, which not only have security concerns, but can be used against you.** (Read more: secaware.co/2n9Scet)
6. **Verify the source of apps to ensure authenticity. With so many in the marketplace, cybercriminals have improved at launching malicious imposter apps.**
7. **Download apps before hitting the road so you're not using data or public networks. And make sure your devices and apps are up to date.**
8. **Turn off Bluetooth and WiFi when not in use. Cybercriminals can sniff out the networks you've connected to before and spoof them (after which your device auto-connects). You might save some battery life in the process!**
9. **Beware of card skimmers. When you need to get cash, it's best to find a bank and use the ATM located inside the building. If that's not an option, carefully inspect the ATM before shoving your card into the slot.**
10. **Beware of smishing. Smishing is a phishing attack via text (SMS) and it's a common social engineering technique. Never click on unsolicited links, and be wary of links floating around on social media.**

Lost Phone? Stolen Phone?

If you're not already familiar, now would be a great time to get to know '*Android Device Manager*' and '*Find My iPhone*'. These remote services allow you to ping your device to ring, change the password or otherwise lock the device, and, in a worst-case scenario, completely wipe the device and restore it to factory default. Remember to always follow policy for work devices. Read more: ***secaware.co/2icj6Uu***.

Good security comes from timely response. Report security incidents immediately!

HEADLINE NEWS

Quick Action Thwarts Ransomware Attack

It's not often we get good news and ransomware in the same headline. But thanks to quick action by a urology clinic with 13 offices based in Texas, we have a success story where ransomware criminals were denied access.

The clinic became aware of the attack almost immediately after it was launched and was able to shut down their network before the ransomware could spread and lock them out of their systems. No ransom ended up being paid. Unfortunately, the clinic couldn't confirm if any personal information had been compromised. As a result, they are offering a year of credit and identity protection to their 279,000 patients.

It may not be a perfect ending, but at least the villain in this story was prevented from carrying out a successful attack, and it just goes to show how important quick detection and incident response are in cybersecurity. Read more here: secaware.co/2nwsZyj.

Internet-connected Dishwasher Found Vulnerable to Hacking.

From the "maybe not everything needs an internet connection" file, we have a report of vulnerabilities discovered in internet-connected dishwashers.

The Miele Professional PG 8528, which is used in medical establishments, has a flaw that allows remote attackers to access directories and steal sensitive information. What makes this situation especially concerning is the environment in which these machines are used. Hospitals store an abundance of personally identifiable information that most go through great expenses to protect.

This is yet another example of how the Internet of Things sometimes does more harm than good. Until better security is implemented by manufacturers, it will be up to end-users to decide whether or not a device should be allowed to connect to a network. In a lot of cases, such as that of a dishwasher, said connection is generally unnecessary. Read more here: secaware.co/2od3XTm.

The Hacker News @TheHackerNews • Mar 22
Russian cybercriminal pleads guilty to developing and distributing Citadel Trojan: secaware.co/2nl3M4w

BBC Tech @BBCTech • Mar 27
WhatsApp's privacy protections questioned after terror attack: secaware.co/2nwitXX

WFTV @WFTV • Mar 27
Data breach may put Daytona State College students' personal info at risk: secaware.co/2nlgb8B

GovTech @govtechnews • Mar 25
Significant Data Breach Impacts Job Applicants: secaware.co/2nHZWbF

Investopedia @investopedia • Mar 27
CIA Used to Hack Factory-Fresh iPhones and Macs per WikiLeaks: secaware.co/2nraFoH

Atlanta Business Chronicle @atlbizchron • Mar 28
Seven lawsuits filed over Arby's data breach: secaware.co/2ndyPBl

The Hacker News @TheHackerNews • Mar 25
Fraudsters using botnet to steal gift card balances: secaware.co/2ocSNOf

HIPAA Journal @HIPAAJournal • Mar 31
Phishing Attack Potentially Impacts 80,000 Patients of Washington University School of Medicine: http://secaware.co/2oRZOI2.

Good security comes from timely response. Report security incidents immediately!