BRIDGEWATER STATE UNIVERSITY
Expect More. Achieve More.

SECURITY Smart™

NEWSLETTER FALL 2016

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

What to Do if Your Files Are Kidnapped

HERE'S A NIGHTMARE situation: Your computer is frozen, your data is inaccessible, and a hacker somewhere out in the ether is demanding you pay up or you'll never see your files again. That's what happens when a computer is infected with ransomware, a type of malicious software that, as the name suggests, effectively kidnaps files and holds them hostage for money. Cybersecurity firm Symantec reports that over the past year, ransomware has reached "a new level of maturity and menace," and the average ransom demand is now $679, up from $294 at the end of 2015.

Signs your device may be infected with ransomware:

- You get a "splash screen" upon startup that prevents you from using the computer and provides instructions on how to pay the ransom to restore access.
- You can't open individual files.
- You notice odd or missing file extensions. Those letters after the dot at the end of a file name (.doc, .exe, .pdf and .jpeg) are the file extension. They let your computer know what type of file it needs to read. Files encrypted by ransomware often have extensions like .crypted or .cryptor or are missing file extensions altogether. In all of these instances, the "finder" tool will display a blank icon for the file type.
- You've received instructions for paying the ransom. The hackers responsible will have left a file with payment instructions. Their ultimate goal is to get paid, so the file should be somewhat easy to find. Look for (but *do not* open) .txt or .html files that begin with an underscore followed by clear language in all caps, such as "_OPEN ME" or "_YOUR FILES HAVE BEEN ENCRYPTED."

If you're hit with ransomware:

- **Try not to panic.** It's natural to freak out when important files go missing or are inaccessible, especially when an unauthorized party is claiming to have the power to destroy them.
- **Disconnect from the Internet.**
- **Don't open the instruction files, and don't pay.** Paying extortion fees only invites more extortion. Payment should be a final, desperate action and only when experts say its your best option.
- **Contact your employer's IT or security department immediately.** They can work with experts to unlock the files and look for the source of the attack.

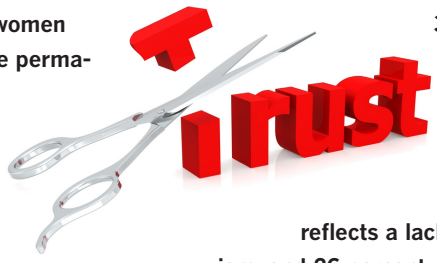
Protect yourself:

- **Practice safe web browsing and email habits.** Don't click on links inside emails, and avoid suspicious websites.
- **Enable your pop-up blocker.** Pop-ups are a popular way to get victims to click on an infected link.
- **Be suspicious of email from unknown senders,** and never click on a link or open or download an attachment unless you're sure you know what it is.
- **Be especially wary of unexpected email from package delivery or postal services,** pop-ups saying you have a virus, email from government agencies (the FBI's name has been used in ransomware scams) and dispute notifications.
- **Keep your software patches and virus protection up to date.**
- **Back up your files frequently** so you won't lose everything if your computer is compromised.

If you have been a victim of ransomware, or any other internet scam, file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov

How We View Companies after a Data Breach

Data breaches have been in the news a lot lately—they've affected organizations big and small, in industries ranging from banking to retail to health care. In the aftermath, companies must scramble to repair not just the damage to their systems, but also the damage to their reputations. That can be a struggle: Nearly one in three Americans said it would take them several months to begin trusting a company again following a data breach, according to a brand perception study recently released by cloud-based encryption company Alertsec, and 17 percent of men and 11 percent of women said their trust would be permanently lost.



"This is no surprise to me," said Ebba Blitz, CEO of Alertsec. "People's personal information is, in many ways, the key to their financial and psychological well-being. When a company has allowed their customers' data to fall into the hands of criminals, the resulting lack of trust is difficult to repair."

Other image problems post-breach: 35 percent of the respondents said a breach reflects sloppiness, 32 percent said it reflects a lack of professionalism, and 26 percent said it makes the company a target for lawsuits. And breaches are unsettling even to people who have no relationship with the compromised company: 97 percent of those surveyed said they are affected in some way, even if they have no direct affiliation.

Hang Up on Phone Fraud

Security columnist Roger A. Grimes, who has written eight books on computer security, nearly fell for a phone scam. He wants you to learn from his close call.

As I landed in Dallas returning from a recent visit to China, I picked up my cellphone voicemails. One of them was from my bank, telling me my personal debit card was frozen and would have to be unlocked.

I knew I should've let my bank and credit card companies know I was traveling, but I hadn't, mostly because I use a dedicated business card when traveling overseas on business. Still, I wondered why this particular credit card was locked. Not only had I not used it on the trip, I hadn't used it in more than a year, and I have multiple credit card security monitoring services that inform me about unusual activity.

I sighed and tried to follow the instructions in the voicemail, but I didn't have time. I had to hit U.S. customs and catch my next flight home. I'd take care of the issue later.

When I got home, I listened to the voicemail message again to get the bank's customer service number. But the voicemail message didn't leave one—the only instruction was to "dial 1 to unlock the card." I hung up and called the number on the back of my card.

To report a stolen card I needed to enter the credit card number, the last four digits of my Social Security number, and some other information I can't remember now. I got a human and told her about my situation. She asked, "Did they call you?" I said yes. Then she asked if they requested that I hit a button to unlock my card. I said yes again.

Then she said: "We don't do that. That was a scam!"

I was floored. Here I am, an overly suspicious computer security guy, but I'm pretty sure if the scammer had reached me directly instead of my voicemail, I would have readily given all the information I was asked for. I was learning that there was yet another scam the world needed to know about.

BUSTED!

The FBI has arrested a U.S. government contractor for allegedly stealing classified documents, possibly including hacking tools.

Harold Martin, 51, was charged in October with stealing government materials. Hard-copy documents and digital information related to the stolen materials, which included two decades' worth of classified materials, were found in Martin's home in Maryland and his vehicle, the U.S. Department of Justice alleged; in addition, authorities allege that he illegally held documents he had no need to see and may have done little to securely store what he allegedly stole. "Many of the marked documents were lying openly in his home office or stored in the backseat and trunk of his vehicle," the filing said.

If convicted, Martin could face 10 years in prison for theft of government property and another year for unauthorized removal of classified materials.

Don't Search for These Stars

Our unending fascination with the lives of celebrities—Brangelina's breakup! Any Kardashian's coiffure update!—often leads us to search online for the latest news and photos. Hackers have learned to take advantage of that predilection, enticing unsuspecting fans to sites that can expose their devices to viruses and malware, or steal passwords and personal information.

Interestingly, some celebs seem to inspire more criminal behavior than others. So which boldface names generated the highest percentage of perilous search results in 2016? According to McAfee's 10th annual Most Dangerous Celebrities study, comedian Amy Schumer is this year's winner. The top 10 are:

1. **Amy Schumer**
2. **Justin Bieber**
3. **Carson Daly**
4. **Will Smith**
5. **Rihanna**
6. **Miley Cyrus**
7. **Chris Hardwick**
8. **Daniel Tosh**
9. **Selena Gomez**
10. **Kesha**

THINK BEFORE YOU CLICK!

Looking for the latest episode of *Inside Amy Schumer*? Don't use that third-party link. Instead, get your content directly from the original source (Comedy Central, at www.cc.com, in this case) to ensure you aren't clicking on anything that could be malicious.

5 Traps Scammers Love to Set

THOUGH WE'VE ALL gotten increasingly tech-savvy, we still keep falling for some basic social engineering scams. Human nature is partially to blame—scammers know how to exploit courtesy, gullibility, curiosity, even apathy. But when you know how scammers work, you can avoid falling into their traps. Here are five hacker favorites to watch out for:

1. **Official-looking emails that appear to be work related,** with subject lines such as "Invoice attached," "Here's the file you needed," or "Look at this resume," often lure unwitting employees into a scam. (*See chart below for a list of the scammy subject lines that get the most clicks.*)

"Most people are not going to look really closely to know where that email came from, and they click on it and their machine may be taken over by somebody, or infected," says Ronald Nutter, author of *The Hackers Are Coming: How to Safely Surf the Internet.*

Be wary of any file that asks you to enable macros, which can lead to a system takeover, and hover your cursor over email addresses and links before clicking to see if the sender and type of file are legitimate.

2. **Messages that say "You missed a voicemail!"** Scammers can install malicious software through emails designed to look like internal voicemail service messages. Businesses often have systems set up to forward audio files to employees, which is convenient, but it can be hard to spot a phishing hoax amid the legit messages.

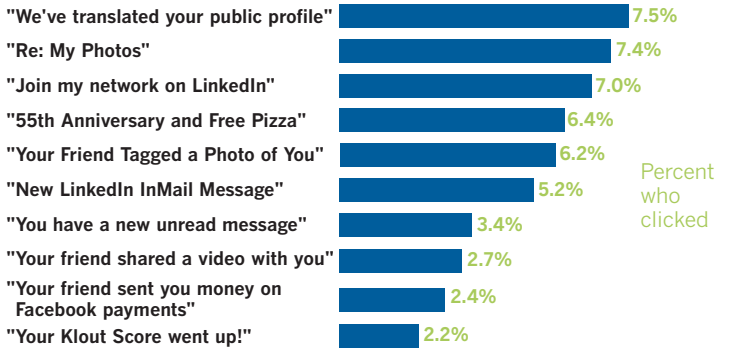
3. **Something for nothing.** Offer people freebies—from pizza to event tickets to software downloads—and they'll click on just about any link to get them, phishing experts say. Stay strong in the face of temptation!

4. **Fake LinkedIn invitations and InMail.** One common scam involves fraudulent employee accounts on LinkedIn that are used for information gathering. For instance, a scammer could create a fake LinkedIn account posing as a known member of your project team or even a company executive. If you accept the invitation and they start communicating with you, you might unknowingly give information that's sensitive or proprietary, and that the scammer can use as part of a broader campaign to gather information about your company.

If you are asked to connect on any social network, email the person's legitimate work address first to confirm they made the request.

5. **If you surf Facebook, Twitter and a host of other social media sites at work,** you are potentially opening the door for cyber thieves. The scams require less work for them: Instead of having to send 1,000 emails to get one hit, they can get people to their page with one post.

This year's most clicked social media scam lines



SOURCE: KNOWBE4

No Walls? No Worries!

Here's how to work securely in an open office space

MORE AND MORE businesses are trading in traditional cubicles and closed-off offices for open floor plans. In fact, the International Management Facility Association reports that 70 percent of American employees now work in open-office environments.

Working in an open office can improve productivity and the ability to collaborate with colleagues, but it also shifts the balance between private and public, and that can pose some security risks. If your job involves working in an open environment, take these precautions to protect your company's confidential information and intellectual property.

1 **Be aware of your surroundings.** Without walls to shield your workspace, vendors, third parties or even malicious coworkers could sneak a peek at proprietary information on your screens or papers. Angle your device screens away from high-traffic areas, shut down and password-protect your computer monitor and mobile devices when not in use, and put away any paperwork containing proprietary information as soon as you're finished with it.

2 **Watch what you say—and where you say it.** In an open office, there's always the possibility of coworkers or outsiders overhearing something they shouldn't. Plan to make sensitive telephone calls or conduct private conversations in a secure space—preferably one with a door.

3 **Keep track of your belongings.** Never leave mobile devices, bags, briefcases, folders or any confidential documents unattended. Instead, opt for secure drawers or other storage areas, and use a laptop cable lock at your workspace.

Free Stuff Can Cost You

What would you do if you came across a bunch of free USB sticks? CompTIA, an IT industry association, recently dropped 200 of them in heavily trafficked public spaces across four major cities: Chicago, Cleveland, San Francisco and Washington. Nearly one in five people who found these random drives proceeded to use them in ways that posed cybersecurity risks (opening text files, clicking on unfamiliar links, or sending messages to a listed email address), thus exposing their personal devices and information, and potentially that of their employer, to hackers. The takeaway? Steer clear of computer-related freebies of unknown origin.

"Tech-Support" Fakers Target People of All Ages

Survey shows younger consumers are most likely to fall victim to their scams

Contrary to conventional wisdom, it's not older consumers who are most easily duped by technical support scams, according to a recent survey, but younger adults. The survey, commissioned by Microsoft, found that people aged 25 to 34 were more than three times as likely to fall for the fake-out as those aged 55 to 64. And the youngest age group, between 18 and 24, were tricked by the scams at more than two and a half times the rate of the group aged 66 and older.

Traditionally, these support scams have relied on cold calls, where phony "technicians" pose as an employee of a company like Microsoft, Dell or HP. The scammer tells a potential victim that his or her computer is infected and tries to convince the consumer or business worker to download software or let the "technician" remotely access the PC. The fraudsters charge for their worthless "help" or sell subscriptions to useless services, and sometimes install malware on PCs while they have the machines under their control.

While older consumers usually experienced these scams by phone—44 percent of those 66 and older said that was how the pitch was delivered—users ages 18 to 24 identified pop-up or online ads as the most common origin (59 percent).

About two-thirds of the respondents had encountered a technical support scam, and about one in five had allowed the scammer to continue his or her story. Nearly one in 10 had actually given money to the fraudster.

What should you do if you get a call or a pop-up message offering technical support? Hang up the phone, and don't click in the box. Microsoft et al. will never contact consumers with those kinds of offers. Anyone who tells you otherwise is trying to scam you.

DID YOU KNOW?

- **94% of employees connect their laptop or mobile devices to public Wi-Fi networks, and of those, 69% handle work-related data while doing so**
- **37% of employees only change their work passwords annually or sporadically**
- **63% of employees use their work mobile device for personal activities**

SOURCE: COMPTIA SURVEY OF 1,200 FULL-TIME U.S. EMPLOYEES

CSO FROM IDG

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