your energy partner®
OPPD
Omaha Public Power District

SHIELD
SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND
Information Protection Newsletter

Review: 2017 Internet Security Threat Report

Below are some highlights of Symantec's 2017 Internet Security Threat Report:

Email
One in 131 emails sent in 2016 contained a malware-laden link or attachment — the highest rate in five years. Malicious email, deemed "the weapon of choice," is "a proven attack channel," reports Symantec. "It doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials." Burgeoning trends in what awaits in your inbox:

Spear-phishing attacks target specific individuals instead of a general, widespread audience (think phishing net). These malicious emails are often disguised as regular emails from trusted sources, such as invoices or delivery notifications. One spear-phishing campaign — fake Google emails instructing targets to reset Gmail account passwords — provided access to the account of Hillary Clinton's campaign chairman John Podesta and resulted in the 2016 presidential election WikiLeaks fiasco.

Business email compromise (BEC) scams, which rely on carefully composed spear-phishing emails, target more than 400 companies each day and have scammed more than $3 billion over the last three years.

Ransomware
Often initiated by email, ransomware attacks increased 36 percent worldwide in 2016 to seize control of person-al computers and institution-wide networks, encrypting hostage files to make them inaccessible until a ransom is paid for their release. Symantec called it "the most dangerous cyber crime threat facing consumers and businesses in 2016." The company identified 101 new "ransomware families" last year, tripling previous numbers.

Another threefold increase: the demanded ransom amount, which averaged $1,077 per victim last year, compared to $294 in 2015. The U.S. is the most targeted and lucrative market, with 64 percent of American victims willing to pay a ransom to regain their files, com-pared to 34 percent globally, Symantec said.

Data Breaches
Although the total number of data breaches decreased last year — 1,209 compared with 1,211 in 2015 and 1,523 in 2014 — they now have a bigger impact. Symantec said that last year, some 1.1 billion identities were exposed, an average of 927,000 per attack; that's twice the 2015 rates on both counts. In 2016, there were 15 individual breaches in which more than 10 million identities were exposed, up from 13 in 2015.

'Smart Home' Devices
With weak factory-issued default passwords that are rarely changed (or can't be), smartphone app-controlled household devices including thermostats, security cameras, door locks, sprinkler systems and even coffeemakers are a worrisome new frontier in computer crimes. Such Internet of Things (IoT) gizmos are already in millions of Americans homes, with predictions that some 50 billion devices will be employed by decade's end.

Already, millions of IoT devices have been hacked, typical-ly enlisted as soldiers in a botnet army that, last October, temporarily knocked offline top websites including Amazon, PayPal, Netflix and Twitter. Some experts suspect this was a test attack to gauge (and prove) their vulnerabilities.

Most often hacked are IoT devices with these passwords, so if you can change them, do so ASAP: "Admin" and "root" lead the list in attempts to log in to the Symantec honeypot (a security technique used to attract swindlers and learn their practices), followed by "123456," "12345," "password," "1234," "admin123," "test" and "abc123." The default password for the Ubiquiti brand of routers — "ubnt" — was also in the top 10, reinforcing the wisdom of having a unique (and strong) password for your home router as well as each smart home device.

https://blog.aarp.org/2017/06/23/new-trends-in-cyber-scams/

STOP. THINK. CONNECT.

STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer

This poster is published by OPPD's Security and Information Protection Department. For more information, please contact us at:

IT-ServiceDesk@oppd.com

Cybersecurity in the Workplace Needs to Be Everyone's Concern

By Susan Hoffman
Contributor, InCyberDefense

Businesses and government agencies are a treasure trove of information for hackers. These organizations store a variety of rich information that hackers find useful, including:

- Names
- Birth dates
- Social Security numbers
- Health insurance member identification numbers
- Credit and debit card numbers
- Phone numbers
- Email addresses
- Intellectual property

With all of this information at their fingertips, hackers can use it to get free medical care or to buy goods or services. In addition, they can steal your identity and get you in financial or legal trouble. Even worse, a hacker can steal your organization's proprietary information to make a profit from insider information or disrupt a company's ability to function.

To prevent future breaches that harm organizations, their employees and their customers, it is vital for *everyone* within that organization to get involved in protecting the cybersecurity of the company. You wouldn't leave your home or office building without locking the doors, right? So you should be equally attentive to "locking up" your company's data through cybersecurity improvements.

In the first half of 2017, over 1.9 billion data records were compromised. (Source: Gemalto)

How Do Hackers Get Access to Company Data?

Hackers enter a computer or computer system in many ways. In the Home Depot hack, for instance, the hackers came in through a third-party vendor. The Target hack involved malware that someone installed on a Tar-get server, which had been taken over by hackers.

In some cases, a hack comes from inside the company. An angry employee who has been terminated, for example, may throw a company's computer system into chaos prior to leaving.

But passwords are still one of the biggest security vulnerabilities. According to Verizon's 2017 Data Breach Investigations Report, "81% of hacking-related breaches leveraged either stolen and/or weak passwords."

Because cyber threats constantly evolve, it is challenging for an IT department to keep up with all the new threats while protecting the organization. But there are ways that other employees and C-level executives can help.

For instance, executives and managers can allocate time for their employees to get cybersecurity training and rec-ognize hacking attempts such as emails (which can be highly convincing at times) that contain links to malware.

Organizations can teach their employees to create secure passwords (a combination of uppercase/ lowercase letters, symbols and numbers) that impede a hacker's ability to guess them. Employees also should check with an IT staff member after receiving a suspicious email or seeing a suspicious website.

Smaller companies are often more popular hacking targets than larger companies, because they have less security and less money for cyber protection. Here, cybersecurity education and training are particularly important. Ideally, all employees and company leaders at smaller companies should have at least some knowledge of cybersecurity to protect the organization from both data breaches and lawsuits from their customers.

Cyber attacks cost companies more than $15 million per year. Although those companies may not want to spend the time or the money to protect themselves, increasing cybersecurity can be a powerful deterrent to many hackers.

https://incyberdefense.com/susan-hoffman/cybersecurity-workplace-everyones-concern/

your energy partner®
OPPD
Omaha Public Power District

PRIVATE INFORMATION IS WORTH KEEPING HIDDEN

- Protect your personal information
- change passwords often
- Lock your computer

CYBER SECURITY IS UP TO YOU!

PRODUCED BY DEFENSE MEDIA ACTIVITY-SAN ANTONIO

VIEW OTHER ART AND PHOTOS AT WWW.AF.MIL

This poster is published by OPPD's Security and Information Protection Department. For more information, please contact us at:

IT-ServiceDesk@oppd.com