CYBERCRIME IS BAD FOR YOUR HEALTH
WHY EVEN SMALL BUSINESSES NEED SECURITY POLICIES
HOW 2FA CAN HELP YOUR COMPANY
5-MINUTE GUIDE TO PASSWORDS
Welcome to the first edition of We Live Security, a magazine which showcases the expertise of security software pioneer ESET, which has been protecting computer users for more than 25 years. Our expertise is showcased online at www.welivesecurity.com in English, German and Spanish. Millions of users around the world now rely on ESET security software to protect their businesses and digital devices, enjoying safer technology through innovation and education.

During more than two decades in the information security industry, ESET has evolved from a pioneer in antivirus software to an award winning provider of multiple security solutions to combat the latest cyber threats. Today’s solutions include ESET Secure Authentication, designed to meet the needs of a workforce who need to safely log into their work network from anywhere, and ESET Mobile Security for Android, offering mobile workers a security solution which not only scans for malware on mobile devices, but also protects against theft and phishing attacks.

Products like ESET Endpoint Security, ESET Smart Security and ESET NOD32 Antivirus are benchmarks for security solutions around the world, providing multiple levels of protection against malware. The ESET LiveGrid global detection reporting system keeps our researchers on top of the latest threats, while heuristic technologies - pioneered by ESET – block emerging threats even before they are widely detected.

It all seems far removed from 1987, when two young programming enthusiasts, Peter Paško and Miroslav Trnka, discovered one of the world’s first IBM PC computer viruses. They dubbed it “Vienna” and wrote a program to detect it. Now, with a presence in more than 180 countries, ESET detects hundreds of thousands of new malware variants a day, and protects users against a wide range of threats, new and old, in a complex world of ubiquitous computing, mobile devices, and constant connectivity. In short, we help the world Enjoy Safer Technology™.

Raphael Labaca Castro
Editor-In-Chief
www.welivesecurity.com

Whether you’re a start-up or a global operation, ESET’s IT security products are fast, easy to use, and deliver market-leading digital threat detection. We deliver the protection that allows you to DO MORE with your business. Find out more at ESET.COM

WELCOME

NEWS AND VIEWS
From ESET’s security experts

STUCK ON WINDOWS XP?
Emergency steps to take

HEALTHY APPROACH
An industry faces new threats

CYBER FIT?
Keep your health data private

WINDIGO: A VICTIM SPEAKS
Cybercrime’s collateral damage

PRIVACY FIRST
For businesses, it’s not a luxury

IN SAFE HANDS
ESET protects SharePoint

SYSTEM ADMINISTRATORS
How to stay friends with yours

WHY YOU NEED CRYPTO
ESET’s encryption solutions

WORLD IMMUNE SYSTEM
How to help fight malware

SECURE AUTHENTICATION
How ESET’s system works

FROZEN WITH FEAR
How scary is the Internet of Things?

WHITE GOODS GONE BAD
Weird tales of fridges gone wild

STRAIGHT TALKING
ESET experts fight back

BUSINESS PROTECTION
8 tips for avoiding big phish...

SCAM-SPOTTER’S GUIDE
How to spot bank fraud attacks

A NEW ROUTE IN
Five tips to secure your router

POLICY DECISIONS
Why clear security policies matter

THE WEAKEST LINK
Passwords: make yours stronger

MOBILE SECURITY
Stay secure on Android

COMPUTER SCIENCE
Why education is the key

STRAIGHT TALKING
ESET experts fight back

POLICY DECISIONS
Why clear security policies matter

BUSINESS PROTECTION
8 tips for avoiding big phish…

THE WEAKEST LINK
Passwords: make yours stronger

MOBILE SECURITY
Stay secure on Android

COMPUTER SCIENCE
Why education is the key
ESET wins Virus Bulletin award

By Raphael Labaca Castro, Editor-In-Chief

In March 2014, ESET’s research team released a significant report on Operation Windigo, for which we were recently given the Péter Szőr Award at the 24th Virus Bulletin International Conference.

The group responsible is using infected servers to send spam, redirect traffic to malicious content and steal more server credentials to widen their campaign. In addition, whenever we find information that provides hints as to the identity of the culprits, we pass it to the police. Commenting on the report, John Hawes, Chief of Operations at Virus Bulletin said, “ESET Canada are worthy winners of this award in memory of the great Péter Szőr. The depth and breadth of the Operation Windigo investigation, the use of a range of groundbreaking techniques, and the high level of collaboration with other researchers and affected parties are all very much in the spirit of Péter’s own excellent work.”

We’ve also collaborated with various international organizations and notified many infected entities to help them clean up their servers. In addition, we’ve been training our customers to recognize and understand the impact of online abuse, including tracking, and action is rarely taken against abusers."

Spyware tracking sees dramatic increase

By David Harley, Senior Research Fellow, ESET

The use of spyware to track a partner’s movements, texts and phone calls is on the rise. A recent survey by UK domestic violence charity Women’s Aid found that 41% of domestic abuse victims had been the subject of harassment using electronic devices or spyware that tracked their movements, calls or texts.

"We increasingly hear stories of abusers adding tracking software to phones, placing spyware on personal computers and using the Internet to gather information about their partner," says Polly Neate, CEO of Women’s Aid. "In many cases the police are not trained to recognize and understand the impact of online abuse, including tracking, and action is rarely taken against abusers.”

Can we predict who will fall for phishing scams?

By Marc-Etienne M. Léveillé

In fact, there’s a great deal of academic literature out there on susceptibility to phishing. What is less clear to me is how you develop a profile while avoiding the pitfalls of stereotyping through over-simplification of social representation.

One idea in a corporate product would be to alert not only the user, but the system administrator, who might recommend training, for instance. In a training tool, risky behavior might be addressed by switching the subject to a different, more intensive module. I’d think that would be compatible with the future research envisaged by the authors of the paper “Keeping Up With the Joneses: Assessing Phishing Susceptibility In An Email Task.”presented by Kyung Wha Hong of North Carolina State University.

User profiling is an interesting approach to countering phishing. But another -- supplementary -- approach would be to analyze the behavior of the PC user and use that analysis to flag risky behavior and attempt some sort of remediation.

The authors of the “Phishing Susceptibility” paper seem to have a profile in mind already. While it’s unsurprising that dispositional trust affects susceptibility to phishing, the study also suggests that gender, introversion and openness to new experiences were also a factor. However, it’s not always clear which way those factors work -- or indeed how representative the population of participants (35 American undergrads aged between 18 and 27) is to the population as a whole. Meanwhile, the phishers keep honing their attacks.

THE TEAM

Three members of the team behind the Windigo paper share their stories.

ALEXIS DORAIS-JONCAS
An ESET employee since 2010, Alexis co-created the ESET Canada office back in 2011 and is currently security intelligence team lead. Alexis lists the Festi botnet as his most hated piece of malware.

MARC-ETIENNE M. LÉVEILLÉ
Marc-Etienne has been a malware researcher at ESET since 2012 and says his biggest Internet challenge is malware that steals money and destroys documents. Which explains his interest in Windigo...

SÉBASTIEN DUQUETTE
A computer science graduate from Université du Québec à Montréal, Sébastien’s golden rule is ‘keep your software up to date’. As a malware researcher for ESET, he says exploit kits are his biggest pet peeve.
How to survive if you’re stuck on XP

By Aryeh Goretsky, Distinguished Researcher, ESET

Millions of PCs around the world still run Windows XP – despite Microsoft no longer providing security updates. If you cannot get away from the old operating system yet, there are things you can do to defend your machines.

The first thing is to make sure you back up your computer’s files regularly, and periodically test your backup strategy by restoring backups – preferably on a different computer – a few times a year. This helps ensure that in the event of a catastrophe, you will have access to your information. The time to worry about your backups is not when faced with a virus, fire, earthquake or other calamity.

Next, make sure that your copy of Windows XP is up to date. Although Microsoft stopped making new patches for the operating system after April 8, 2014, all of the old updates from before then will still be available, and should be downloaded. This also applies to the device-driver software (a device driver is a computer program that allows the operating system to communicate with a particular kind of hardware), which may be available from your computer manufacturer or Microsoft’s Windows Update Website.

You should also make sure you have the latest versions of the application software on the computer, and that these are fully patched and updated. Software like Adobe Flash, Adobe Reader and Oracle Corp’s Java are frequently targeted by criminal gangs who develop and use malware, so keeping these up-to-date is just as important as looking after your operating system. Other software that you use, such as Microsoft Office, Web browsers and so forth, should be on the newest version and have the most recent patches applied as well.

If you don’t need the Web, disconnect or disable the connection so that the PC can only connect to other machines on the same non-Internet network. This will ensure that Internet-borne threats cannot directly attack your XP PC, and will make it harder for an attacker to steal data off the computer.

Make sure your security software is up to date, too. There are lots of security programs available for Windows XP, and most of their authors have committed to supporting the operating system for years to come. Some are free, while others are sold as a subscription. A discussion of the features needed to protect Windows XP is outside the scope of this article, but at the very least, I would recommend a personal firewall and exploit blocking will be useful, too, as Windows XP will no longer be updated by Microsoft to protect against these types of attacks.

ESET crossword

Across

1 Perform before most important section of network or Web (6)
2 APT targeting Google, Yahoo et al is hiding back in Qatar or UAE (6)
3 Stutterer’s precursor to Windows that leads to combined bandwidth flooding (4)
4 See 12 down
5 Spare 2k confused mass-mail sender (9)
6 Various ways to be social online, but all I hear is, “Myself! Precious!” (9)
7 Non-public posting gets around, first read in secret, then snooping project revealed by NSA leak (5)
8 Hippos enjoy having drunkard around in Linux server-targeting operation? (7)
9 Not from round here, and not feeling well! Sounds like this sort of analysis might get to the bottom of things (8)
10 Turbo Python hides reversing keyboard error (4)
11 Retailer leaking masses of data, as shown by that rogue UTM, oddly (6)
12/10 Endpoint traffic filter has intimate knowledge of a private network section or Web (6)
13 Various notches (6)
14 Computer firm in the trash can – malware may try to steal yours or mine (7)
15 Slackware, Edubuntu and Gentoo provide initial braces for low-tech snow vehicle (7)
16 Disassembly expert type examines code, then starts to spot malware (6)
17 External drive connection is at sea, all at sea (5)
18 Fellow to look for node-linking architecture, shortened (7-7)
19 Revealed by NSA leak (5)
20 To surf the Web, plumber’s enemy has to shift his bottom up a few notches (6)
21 FIFTH ELEMENT – going for a gentle walk, first off, then lurking online to annoy others (8)
22 Computer threat, a type of virus (6)
23 To give a gentle walk, first off, then lurking online to annoy others (8)
24 Computer threat, a type of virus (6)

Down

1 Round off-egg-shaped function, which returns no value (4)
2 Freak NMS worm; even you will pay this to rescue kidnapped data (6)
3 After college, put away documents left out, then joined up, as seen in multi-function appliance (6)
4 Apple system connects to East European TLD, an old hiding place for document threats (6)
5 To surf the Web, plumber’s enemy has to shift his bottom up a few notches (6)
6 Going for a gentle walk, first off, then lurking online to annoy others (8)
7/8 Personal firewall
8 Computer threat, a type of virus (6)
9 Internal drive connection is at sea, all at sea (5)
10 Fellow to look for node-linking architecture, shortened (7-7)
The growing threat to the security of our health data

By Brad Tritle, global product owner for Vitaphone Health Solutions and co-founder of eHealth Nexus

For 2015, there are three areas of health IT security (and privacy) that I believe will be taken much more seriously than in the past: HIPAA training (an American law that helps to guarantee security of health data for patients), role-based access and security of mobile device applications.

Anyone who has worked at either a HIPAA-covered entity or business associate has undergone some form of HIPAA training, and then signed an agreement indicating that they have been trained and will comply with HIPAA, with intentional non-compliance serving as cause for release from employment.

When I served on The Office of the National Coordinator’s Health Information Security and Privacy Collaborative (HiSPC) several years ago, we found that most healthcare providers erred on the side of doing more than HIPAA required from a privacy perspective. Since that time, however, security requirements (e.g., HITECH) and associated threats have increased. Meaningful Use (MU) has both required performance of HIPAA security audits for those wanting their MU payments, and created a marketplace where other organizations, such as HIPAA Business Associates, can more readily perform such audits. The result: stronger security guidelines are being put in place across the industry, and employees will be required to not just sit through a 30-minute video, but to be thoroughly trained and tested on specific employee requirements that will facilitate the organization’s HIPAA compliance.

Role-based access, or the ability for a healthcare professional to have only access to the protected health information for which he is authorized (e.g., a treating physician looking at the record of the patient under their care), is going to become more granular. Many in-patient, ambulatory and payer systems have facilitated a single user having practical access to any patient record on that system, regardless of whether there was a reason for that user to access that record. It is only if and when unauthorized access is discovered (which is becoming more frequent), post-event, that discipline can occur. This same issue can occur with query-based Health Information Exchange. Moving forward, there will be increased use of consent engines to ensure a system not only complies with unique geographical privacy and security regulations, but also that only those with a true need to access a record can do so.

One of the biggest trends in healthcare is the increased use of mobile devices, both for providers and patients. There are tens of thousands of health apps available to patients, and the number is increasing. In parallel, health care providers, such as hospitals, are sending patients home with mobile devices for remote patient monitoring, in order to reduce the need to re-admit them to hospital. Though theoretically the patient could download an app, what we are seeing is the provider’s provision to the patient of a separate, locked-down, mobile phone that serves a single purpose, for example, a mobile gateway for a blood pressure monitor. This prevents potential misuse of the phone (stories of patients calling their family in a foreign country on a provider’s phone do exist), but also ensures the security of the data—either in the hands of the patient, or should the patient misplace the phone. This additionally aids the patient by ensuring that data transmission costs are not billed to her personal account. Will this change in the future? Undoubtedly, and it is also an opportunity for companies to develop new mobile health security solutions.

One of the biggest trends in healthcare is the increased use of mobile devices, both for providers and patients.
Healthcare: new cyber risks

From doctors using smartphones at work to connected devices with password vulnerabilities, there are numerous cyber risks facing the health industry.

Heart defibrillators face cyber attack
In 2013, the risks of ‘connected’ healthcare devices were shown off starkly in America: 300 gadgets – including heart defibrillators and patient monitors – had dangerous password vulnerabilities that could have been exploited by cyber attackers, according to the Food & Drug Administration (FDA). “The vulnerability could be exploited to potentially change critical settings and/or modify device firmware,” it warned.

Medical data – is it secure enough?
The Identity Theft Resources Center claims that the medical industry accounted for 4.3% of all data breaches in 2014. ESET senior researcher Stephen Cobb says, “Healthcare has seen rapid growth in the use of digital systems. But despite a regimen of rules aimed at safeguarding the privacy and security of patient data, in the US the sector is currently rife with security breaches.”

Medical phishing: a new frontier
Cybercriminals have become smarter at impersonating banks, but new phishing campaigns use cancer scares to target victims. Emails purporting to be blood-test results go on to infect computers when opened. In one campaign in Britain, the National Institute for Health and Care Excellence (NICE) said, “We’re aware a spam email is being sent regarding cancer-test results. This email is not from NICE. If you have received the email, do not open the attachments.”

Leaks can damage your health
Security issues that lead to information about medical conditions leaking can cause serious financial and emotional harm – and researchers have found that even ‘secure’ browsing may not be private. They revealed a technique for identifying individual Web pages visited ‘securely,’ with up to 89% accuracy, exposing data such as health and financial details and sexual orientation.

TIPS FOR protecting your medical data

By Lysa Myers, Security Researcher, ESET

Do not share personal details unless you absolutely have to Do not share personal details unless you absolutely have to. A lot of fraud happens because people give their login or insurance information to friends or family members. If someone gets medicines under your name, it will be listed for you and may mean you get improper medical care. Or you could end up having to pay someone else’s bills.

Check your statements Be sure to read thoroughly and understand the charges that come in your statements from doctors’ offices and insurance companies. If you do not understand what you see, or if you see something listed that you do not recall having been done or given to you, call back and get an explanation.

Check your apps and health data If you use an app to track health data, it’s a good idea to see how well it safeguards your information. Reviews online and at the app store where you bought it or go to a good place to start. Check the permissions for the app to see what other information it may be accessing. You can encrypt data on your mobile device for extra protection.

Advocate for security and privacy If you feel comfortable discussing security measures and privacy controls, ask your health providers what measures they have in place to protect your data. You might be surprised at the answer – and not always for the worse. Many healthcare practitioners I’ve spoken with have well thought-out security in their environments.

REGARDS DIGITIZING ALL PATIENT HEALTH RECORDS

41% would not support the move toward digitizing all patient health records in the US.

REGARDING SECURITY AND PRIVACY OF ELECTRONIC PATIENT DATA

40% are concerned about the security and privacy of their electronic patient health records.

17% say this is not applicable to them; their health records are not in electronic format.

HEALTH PRIVACY: ARE WE WORRIED YET?

43% of Americans familiar with the NSA revelations are not concerned about the security and privacy of their electronic patient records. Those aged 25-34 (46%) are more likely than those aged 18-24 (36%) to not be concerned about this. And those with a household income of $75k or higher (48%) are more likely to say this.

17% of Americans familiar with the NSA revelations say that to their knowledge, their health records are not in electronic format. Interestingly, those aged 18-34 (27%) are twice as likely than those aged 35+ (13%) to believe their health records are not in electronic format.

Source and survey methodology: The survey was conducted online within the United States by Harris Poll on behalf of ESET from February 4-6, 2014 among 1,691 U.S. adults aged 18 and older, among which 43% are at least somewhat familiar with the NSA revelations.

Images: ©Rex Features

HEALTHCARE:
Are YOU SAFE?
41% of Americans are concerned about the security and privacy of their electronic patient health records.

Medical implants could be targeted
Security Protection Alliance claim that Center and the International Cyber Alliance claim that Center and the International Cyber War ‘inside the human body’

Could become targeted
Heart defibrillators and patient monitors – could be targeted.

Security Protection Alliance claim that Center and the International Cyber War ‘inside the human body’

Cancer-test results go on to infect computers when opened.

The Identity Theft Resources Center claims that the medical industry accounted for 4.3% of all data breaches in 2014.

ESET senior researcher Stephen Cobb says, “Healthcare has seen rapid growth in the use of digital systems. But despite a regimen of rules aimed at safeguarding the privacy and security of patient data, in the US the sector is currently rife with security breaches.”

“Secure” browsing may not be private.

You can encrypt data on your mobile device for extra protection.

Should we be ‘appy’ when doctors bring their own?
Most hospitals now permit clinicians to BYOD – bring your own device – to the workplace. PwC’s Top Health Industry Issues 2013 report said that 85% of hospitals allow this. Just last August, the United States Computer Emergency Readiness Team released a statement saying it was aware of a breach of sensitive patient identification information affecting some 4.5 million patients.

But despite a regimen of rules aimed at safeguarding the privacy and security of patient data, in the US the sector is currently rife with security breaches.”

Medical phishing: a new frontier
Cybercriminals have become smarter at impersonating banks, but new phishing campaigns use cancer scares to target victims. Emails purporting to be blood-test results go on to infect computers when opened. In one campaign in Britain, the National Institute for Health and Care Excellence (NICE) said, “We’re aware a spam email is being sent regarding cancer-test results. This email is not from NICE. If you have received the email, do not open the attachments.”

Leaks can damage your health
Security issues that lead to information about medical conditions leaking can cause serious financial and emotional harm – and researchers have found that even ‘secure’ browsing may not be private. They revealed a technique for identifying individual Web pages visited ‘securely,’ with up to 89% accuracy, exposing data such as health and financial details and sexual orientation.

TIPS FOR protecting your medical data

By Lysa Myers, Security Researcher, ESET

Do not share personal details unless you absolutely have to
Do not share personal details unless you absolutely have to. A lot of fraud happens because people give their login or insurance information to friends or family members. If someone gets medicines under your name, it will be listed for you and may mean you get improper medical care. Or you could end up having to pay someone else’s bills.

Check your statements
Be sure to read thoroughly and understand the charges that come in your statements from doctors’ offices and insurance companies. If you do not understand what you see, or if you see something listed that you do not recall having been done or given to you, call back and get an explanation.

Check your apps and health data
If you use an app to track health data, it’s a good idea to see how well it safeguards your information. Reviews online and at the app store where you bought it or go to a good place to start. Check the permissions for the app to see what other information it may be accessing. You can encrypt data on your mobile device for extra protection.

Advocate for security and privacy
If you feel comfortable discussing security measures and privacy controls, ask your health providers what measures they have in place to protect your data. You might be surprised at the answer – and not always for the worse. Many healthcare practitioners I’ve spoken with have well thought-out security in their environments.

REGARDS DIGITIZING ALL PATIENT HEALTH RECORDS

59% would support the move toward digitizing all patient health records in the US.

REGARDING SECURITY AND PRIVACY OF ELECTRONIC PATIENT DATA

40% are concerned about the security and privacy of their electronic patient health records.

17% say this is not applicable to them; their health records are not in electronic format.
How my firm fell victim to cybercrime

Windigo victim speaks out on the ‘stealth’ malware that attacked his global company

Operation Windigo was one of the biggest criminal operations of 2014. The counterattack is being led by ESET employees – who created an award-winning white paper on Windigo – with help from law enforcement and scientists from around the world, including Europe’s CERN, the organization behind the Large Hadron Collider. The paper highlighted a dangerous threat, where criminals target UNIX servers to redirect victims – and take over thousands of servers and sites worldwide.

The gang used these servers to send spam, redirect Web traffic to malicious content and steal more server credentials to widen their operation. At its height, Windigo sent 35 million spam emails a day and redirected 500,000 Web users to dangerous sites. Detailed analysis of the attack – and ESET’s action against it – can be found on ESET’s news and opinion hub welivesecurity.com.

ESET researchers have helped many companies identify and neutralize the infection. Francois*, owner of a business whose servers in France and Canada fell victim for weeks, explains how even a large Internet firm can fall prey to an attack – yet not notice.

Were you aware that this sort of attack was possible?
"To begin with, we didn’t realize what it was. But this did not feel like something really offensive. It was running in the background pretty silently – no crashes or anything. I think that’s why it has infected so many servers before people reacted."

Did the nature of the attack surprise you at all?
"One of the first things you learn in any form of high-tech business is that anything is possible. But we knew from the start that Windigo was something different. It was subtle. No one stole our database – the first we heard was when suspicious behavior was mentioned by some of our customers."

How did you react? Did you fear your business was under threat?
"We rapidly went from not worrying to the worst worry of all – that it was an advanced threat, targeted at us. We have a lot of servers, and many customers in France and Canada. We quickly realized that plenty of people were talking about those strange behaviors on many forums."

Did you work closely with researchers on this?
"We were quickly contacted by ESET and were told about how big this infection was and started to work very closely with their research team. We cleaned infected servers but kept some intact for ESET’s investigation. Marc-Etienne Léveillé of ESET offered some really good advice – clean the server and reinstall. It’s a harsh cure, but we did it. Thanks to the quick action of ESET, our company’s reputation was not damaged – we listened to our customers and acted. We did not suffer severe financial loss, either."

What are your feelings towards the gang who created this attack – and the companies still suffering form its harsh effects?
"This attack is big. Many Web hosting companies were infected and didn’t even know what it was. We were lucky in the end. We worked closely with ESET, who helped put it right, and I hope we helped in turn with the Windigo project."

What is the status of your company now that you have survived the attack?
"We are fully operational. If the government took these kind of attacks more seriously and invested more money to help companies such as ESET, it may prevent more damage."

*At his request, We Live Security used a pseudonym for our interviewee.

Do More when you have secure access to your data

• Ultra-strong ID validation for use with mobile, tablet or your existing hardware tokens
• A powerful, simple solution
• Two-factor authentication, using one-time passwords

ESET SECURE AUTHENTICATION

ENJOY SAFER TECHNOLOGY™
Why privacy is on everyone’s mind in 2015

By Stephen Cobb, Senior Security Researcher, ESET

Last year’s ESET Threat Report demonstrated that online privacy had become something the world was worried about in the wake of Edward Snowden’s revelations. I predicted an unprecedented level of interest in encryption products due to continuing revelations about state-sponsored surveillance of companies and consumers.

Privacy has become a luxury — for example, biometrics are built into the most expensive smartphones and PCs. I predict a small but not insignificant percentage of current Internet users in developed countries will scale back their online activities in light of continuing revelations about state-sponsored surveillance of companies and consumers.

For businesses, it’s not a luxury. It’s an essential. All employees need to be made aware of the company’s privacy policies (assuming you have these properly documented). Today’s smart companies are making sure that every employee who deals with customers’ personally identifiable information, even the folks in IT whom you might not think of as “customer” people, are aware of just what a big deal it is to breach the privacy promises that the company has made to its customers.

Any transgressions that come to the attention of management should be addressed (this may not mean firing people — but if you don’t enforce a policy it is legally useless in your defense).

I will close by quoting J. Howard Beales, III, Director of the FTC’s Bureau of Consumer Protection.

Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information.

Privacy 101: Why changing privacy settings is essential

Many users of sites such as Facebook don’t change privacy settings at all, unaware that the site’s powerful Graph Search can leave their personal information exposed. Here are three crooks who must wish they had changed theirs...

Just stole these rings LOL

A jewel thief stopped off during a robbery for a less-than-essential break — to check Facebook (his own, real account) on the victim’s laptop. Walking out with two diamond rings worth $5,500, he was swiftly arrested and jailed.

Just robbed a bank? Time for a selfie!

Sure, selfies are in vogue — but the Michigan bank robber who posted a photo on his Facebook page, with a submachine gun of exactly the same make used in the hold-up, may have regretted his “Bought my first house and chopper today life’s great.” he said. If that isn’t a reminder to change your privacy settings, what is?

‘Catch me if you can’

A criminal who taunted police with a Facebook message saying “Catch me if you can” was caught 12 hours later. The 19-year-old, on the run from prison, was caught after police appealed on Facebook for information, and he posted his taunt on the page. The information it revealed was enough to catch him — and earn him 10 months in prison. “Caught you,” the police posted.

SharePoint is seen as a must-have for many organizations around the world. This collaboration software from Microsoft provides a place to store, organize, share, and access information from virtually any device. The only requirement is a Web browser.

While Microsoft SharePoint Server 2013 brought many improvements, it still requires an additional security layer to safeguard sensitive company data, as well as assets stored in databases.

ESET Security for Microsoft SharePoint Server provides real-time protection for SharePoint servers and databases. Over and above protection against cyber threats — including those aimed at file system entry, drive-by downloads, system exploits and vulnerabilities — ESET’s server technology includes password protection to stop both malware and unauthorized administrators from disabling it. ESET scans everything in the database, and protects the server as well as its content.

While most server-based security software products have a noticeable impact on system resources, ESET’s security offerings are recognized by industry testers and analysts around the world as having a very small footprint with minimal impact.

ESET Security for Microsoft SharePoint Server is no exception, operating efficiently without noticeable impact on server performance. It excludes critical server files automatically, so applications like Microsoft SQL Server and Microsoft IIS are recognized and omitted from the scans.

Another feature to speed up scanning time is its rule-based filtering, which lets administrators fine-tune protection by specifying file name, size and real file types.

ESET Security for Microsoft SharePoint Server also detects server roles. By excluding critical server files like data stores and paging files from on-access scanning, ESET Security for Microsoft SharePoint Server has a much lower system impact than the competition.
The secret to a harmonious relationship with your system administrator

By Carole Thériault, Director, Tick Tock Social

Being a great IT administrator (or sysadmin) can seem impossible these days. This is a real shame, because having a good sysadmin can make a huge difference to the bottom line: when optimized systems run smoothly, work gets done more efficiently, saving time and money.

So why this massive disconnect between the IT team and the rest of the business? This situation can cripple a business in today’s fast-paced, competitive market. The solution is a question of shifting perspective just a little, along with a touch of empathy and a bit of new strategy.

First, we need to get into the heads of sysadmins, and understand their relationship with the people they consider their customers (the rest of the organization).

Why life is now tougher

A sysadmin is hired by a company to make sure that all computers, devices and servers, as well as all the software installed, work reliably. Twenty years ago, when most people relied on desktop systems running Windows and MS Office, life was much simpler. Mobile phones had also not made an appearance. As all the software installed, work reliably.

The vast majority of sysadmins don’t possess in-depth knowledge of the systems they use. It is similar to owning a car: you want it just to work, and when it doesn’t, you want to take it to the garage and get it fixed.

Explaining the disconnect

The daily grind of maintaining systems for people who are not inclined to understand how they work or what breaks them, sprinkled with zillions of urgent requests to fix connectivity, access, privacy, printer, application, server and device issues, would be enough to make anyone a little grumpy.

From a user perspective, sysadmins are the people who are never at their desks when you call upon them, who look at you placidly and give you a ticket number even when you label a request as urgent, and who ask lots of questions you cannot answer, like “what version of OS and browser are you using?”

Appreciate resource restrictions. Your IT team need to prioritize where they put their time, and in order to get your problem sorted, you need to simplify the task for them and explain clearly what impact the issue is having on business continuity.

Be prepared. Sysadmins are not wizards. They need to diagnose the problem. Help them with this. Always bring your computer ID information, operating system version, any application version numbers that are causing difficulty, screenshots of a problem, and details of what you tried and how you performed the actions.

Time your approach. Monday mornings are often hellish for system administrators. They need to resolve all the issues that their customers had over the weekend. If your problem is not extremely urgent, save it for another day.

Don’t bypass protocol. Of course you might have identified a faster route to get your problem fixed (via a manager, for instance) but this can disrupt the entire ecosystem. Save that route for extreme emergencies, and help IT create a system that works.

FOR CUSTOMERS:

Show respect. A sysadmin’s job demands multitasking and extreme focus, which is exhausting. Every time you show up with a query, apologize for the interruption and request assistance politely.

Appreciate resource restrictions. Your IT team need to prioritize where they put their time, and in order to get your problem sorted, you need to simplify the task for them and explain clearly what impact the issue is having on business continuity.

Be prepared. Sysadmins are not wizards. They need to diagnose the problem. Help them with this. Always bring your computer ID information, operating system version, any application version numbers that are causing difficulty, screenshots of a problem, and details of what you tried and how you performed the actions.

Time your approach. Monday mornings are often hellish for system administrators. They need to resolve all the issues that their customers had over the weekend. If your problem is not extremely urgent, save it for another day.

Don’t bypass protocol. Of course you might have identified a faster route to get your problem fixed (via a manager, for instance) but this can disrupt the entire ecosystem. Save that route for extreme emergencies, and help IT create a system that works.

FOR IT ADMINISTRATORS:

Adopt the Bozo rule. Sadly, many sysadmins cannot do it all. Keep the masses and influencers (your boss, the CEO, and the worker bees) as happy as possible. Prioritize work by thinking in terms of the health of the business, not the person who shouts loudest or annoys you most. And keep a list of your actions, so if anyone complains, you can prove you made the right decisions.

Keep control. You are your company’s IT guru. Ooze quiet calm, knowledge and confidence in the same way you would want your doctor or dentist to.

Lose the attitude. Yes, you absolutely have a seriously tough job, but so do others. Earn respect whenever possible, but don’t force people to understand your challenges and frustrations.

Don’t show off. Learn how to explain solutions in everyday language. The more educated your customers are, the easier your job will be in the long run. Who knows? They might even fix the printer jam themselves!

Explain why the answer is no. Sysadmins are often accused of being negative and dictatorial. Always try to provide a clear explanation as to why you cannot provide a service.

FOR CUSTOMERS:

Show respect. A sysadmin’s job demands multitasking and extreme focus, which is exhausting. Every time you show up with a query, apologize for the interruption and request assistance politely.

Appreciate resource restrictions. Your IT team need to prioritize where they put their time, and in order to get your problem sorted, you need to simplify the task for them and explain clearly what impact the issue is having on business continuity.

Explain why the answer is no. Sysadmins are often accused of being negative and dictatorial. Always try to provide a clear explanation as to why you cannot provide a service.

FOR IT ADMINISTRATORS:

Adopt the Bozo rule. Sadly, many sysadmins cannot do it all. Keep the masses and influencers (your boss, the CEO, and the worker bees) as happy as possible. Prioritize work by thinking in terms of the health of the business, not the person who shouts loudest or annoys you most. And keep a list of your actions, so if anyone complains, you can prove you made the right decisions.

Keep control. You are your company’s IT guru. Ooze quiet calm, knowledge and confidence in the same way you would want your doctor or dentist to.

Lose the attitude. Yes, you absolutely have a seriously tough job, but so do others. Earn respect whenever possible, but don’t force people to understand your challenges and frustrations.

Don’t show off. Learn how to explain solutions in everyday language. The more educated your customers are, the easier your job will be in the long run. Who knows? They might even fix the printer jam themselves!

Explain why the answer is no. Sysadmins are often accused of being negative and dictatorial. Always try to provide a clear explanation as to why you cannot provide a service.
What’s the problem?
A company without data is unimaginable. Data is the lifeblood of your business – it needs to flow safely between different parts of your organisation and between team members collaborating on a project. You cannot afford to lose any of it.

And there are many ways for data to be shared: via email, shared folders, USB sticks, cloud-storage services, laptops and CD ROMs… the list goes on.

The danger is that the movement of data poses a big risk for enterprise. As it travels between users and outside the company, it could either be leaked accidentally to unauthorized parties or intercepted and stolen by malicious hackers.

Furthermore, sensitive information and databases stored on your corporate servers – if not protected properly – might be a tempting target for cybercriminals and online thieves.

Barely a day goes by without an organisation becoming the unwelcome recipient of newspaper headlines announcing that customer data (such as credit card details, passwords or personal information) has been stolen.

It has become clear that the danger is not just one of losing data related to your customers but of losing their trust to such an extent they no longer want to do business with you.

What’s the solution?
ESET provides encryption solutions which enable organizations to secure data.

Centralized policy management makes it easy to manage users and workstations and extend the protection of your company beyond the perimeter of your network. Encryption security can be painlessly rolled out, and even extended to mobile phones and home users.

Even if encrypted data falls into the wrong hands or is contained on a device accidentally lost by an employee, your business can feel confident that the sensitive information will not be exposed.

Business benefits
● Full disk and removable media encryption protects data stored or sent using laptop computers.

● File, folder and email encryption enables fully secure collaboration across complex work groups and team boundaries.

● Security policy enforcement deployable at all endpoints.

● A single MSI package meets data security compliance obligations.

● Uniquely patented security key management allows full control of encryption keys and encryption security policy remotely and silently.

● Patented hybrid cloud architecture means that all client and server connections are SSL encrypted, and all commands and data are AES or RSA encrypted.

● Quick install and low system requirements bring enterprise-grade security to even the smallest organisations.
IT security software isn’t a program in your hard drive – it’s a communication system. Done right, it works like an immune system, but a global one.

When I first started working for an IT security company in 1992, you’d get your software updates on floppy disks. They were sent out every three months. If you were really paranoid, you went for the monthly updates. Viruses took months to spread around the world – via floppy disk. There were 200 new viruses a month – and we thought that was pretty bad.

Now, of course, we see 100,000 new variants of malware a day. As soon as money became involved, it became industrialized – and I have to say, some of the fun went out of being a virus researcher.

Back in the old days viruses weren’t made to make money – they were just graffiti. They could cost you money – but the point would be the letters falling down your screen, or a graphic of an ambulance driving across. There was an artistry there – something I blogged about a while ago.

Many viruses were also unique – even if they were destructive. I remember a polymorphic infection from the early days – where the writer was so keen to make a British piece of malware. The SMEG Pathogen virus, named after a crude word used in the British TV comedy show Red Dwarf, was written by this English chap Christopher Pile. It stood for Simulated Metamorphic Encryption Generation. When it wiped your hard drive, it said, “Smoke me a kipper, I’ll be back for breakfast... but your data won’t.”

The media had been guilty of presenting malware as largely Eastern European in origin, and Pile wanted to prove them wrong. With the commercialization of malware, that’s all gone. They don’t care about the quality – just the money. I saw it first with attacks targeting AOL users. They were stealthy – just stole password details and credit cards.

There wasn’t any attempt to be clever. There were enough people who didn’t update Windows that it would spread anyway. Now, it’s more than that. It’s “let’s write computer programs to write more malware for us”.

Spotted by computer

But now, most of what we see is not entirely new and unique. It’s based on malware we’ve seen before. Each new variant has been written by a computer – and is usually spotted by a computer.

Even if you have 100 researchers, you can’t keep up with the volume of detections. Expert systems do the detection – customers want protection very, very quickly, and humans can’t provide that level of speed and accuracy. Expert systems can.

An expert system can, for instance, look inside a piece of code, and make a guess about whether it’s a banking Trojan very quickly. They’ll scan for banking URLs – or related ones. They’ll look for other markers – is there any Portuguese? A lot of today’s banking Trojans come from Brazil – and the code’s compiled with Delphi. So the system will look for a Delphi copyright message – but of course, the cybercriminal knows it will, so he’ll write that it was done in Microsoft C. A clever expert system will look at that and know that here we have a piece of code that’s in Portuguese, is pretending to have been compiled in C – hiding its origin – and has banking URLs in it. Even if you’ve never seen it before, you’ve already got a good idea it’s bad.

That’s a very simplified take, of course, but this proactive defense is the future. Not in labs, but in home PCs. You have to look at the behavior of malware in real time, and when you think, “This is suspicious”, either turn it off, alert the user, or report back to base. Your PC has to be part of a bigger system.

IT security software isn’t a program in your hard drive – it’s actually a communication system. Done right, it works like an immune system, but a global one. Sending information isn’t always something we like to do. Those windows asking you to share information are needed more than ever.

“We’re all on the Internet, which means we’re all part of the same family. It’s up to all of us to defend it.”
POWER UP YOUR PASSWORDS

We Live Security’s experts explain how we work to keep you and your business safe

WHAT’S THE PROBLEM?

More and more organizations are becoming aware of the risks posed by sloppy password security.

Most network intrusions (86%) are attributed to hackers exploiting weak or stolen login credentials such as passwords - so it is clearly a problem any business should deal with. Failure to do so means workers might create their own passwords which are either not random enough or easily guessable, opening opportunities for hackers to exploit their accounts.

In addition, many computer users make the mistake of using the same password in multiple places, such as using a password from inside the corporation for a private account.

In that scenario, if a user’s password is compromised elsewhere, it could lead to a breach of your own company’s systems.

And, of course, if just one employee has their password phished or hacked, online criminals could gain direct access to your corporate network or company secrets.

Computer users cannot be relied upon to always create strong, hard-to-crack passwords, or to protect them effectively from falling into the hands of cybercriminals.

Fortunately, technology can help with the problem.

Secure authentication can make remote access to a company’s network safe and hassle-free.

ESET Secure Authentication introduces a two-factor, one-time password into your users’ login process, meaning that if their regular password is guessed, cracked or stolen, hackers will not be able to gain access to your most sensitive information.

This works like this. Employees, upon remotely accessing the company network, receive a one-time password on their mobile phones, either via an app or, if the app is not installed, via SMS. After its initial set-up, the app does not require internet access.

This password is then used to strengthen the usual authentication process. And because the one-time password is unique, and is delivered to the employee’s mobile phone, hackers cannot ‘steal’ it. As a result, the company data and assets are protected against intruders, dictionary attacks, password guessing and the other methods hackers use to gain access to business networks.

ESET Secure Authentication Software Development Kit has a range of extensibility options, allowing you to add two-factor authentication to nearly any system that requires authentication.

ESET SECURE AUTHENTICATION SOLVES THESE PROBLEMS:

Static passwords that can be intercepted

User-created passwords that can be easily guessed

Re-use of private passwords for company accounts

Passwords containing user-specific data – e.g. a name, a date of birth

Simple patterns to derive new passwords, such as ‘peter1’, ‘peter2’, etc.

BUSINESS BENEFITS

Helps prevent the risk of breaches with unique passwords for each access

Protects from poor password practices

Saves costs - no additional hardware needed

Easy to migrate to and use

Two-factor authentication provides peace of mind

Multi-platform support, including leading mobile operating systems

Global technical support in local languages

LOW HANGING FRUIT

Small to Medium sized Businesses: The Cybercriminals’ Sweet Spot

66% of breaches are undetected for months, increasing the potential damage!

$224 Average cost per incident

$153 Average cost per incident

WEAK PASSWORDS

#1 Risk to IT Security: Stolen Password

Tips for Stronger Passwords

str0ngPassSTOPhak3r3l

Combine lower & upper case, numbers and symbols

Use more than 8 characters (better to combine words, 10-16 characters)

Change your password more than once per year

OUTSMART HACKERS

With Two-Factor Authentication (2FA)

2FA validates identities & keeps data secure

This infographic was created by ESET, a maker of security solutions. Check out our 2FA solution – ESET Secure Authentication at www.eset.com

References

Kaspersky’s Data Breach Report 2015

PasswordAttribute, 2015 Cost of Data Breach Study, Gartner

IDF Information Security Research Group, The Department for Business, Innovation and Skills (BIS) and PwC

CISO Cybersecurity Password Habits (2012)
ESET ENDPOINT SECURITY FOR ANDROID

Mobile security has and always will be a pressing issue for companies everywhere. Businesses striving for success rely on an operating system to function seamlessly from a security standpoint.

ESET Endpoint Security for Android is the solution for all your data security needs. With Android’s increasing popularity, there has never been a stronger emphasis on mobile security. With improved usability and effortless navigation, ESET Endpoint Security for Android is yet another example of ESET’s drive to become a primary contender in the market for business security solutions for Android-based devices.

ESET Endpoint Security for Android gives administrators complete control over installed applications, allowing blocking based on a manually defined list, or based on categories or source of the application.

In addition to fine-tuned application control, ESET Endpoint Security for Android allows admins to set minimum security levels across multiple devices — with variables such as minimum password length or number of upper/lower-case letters required — for fine-tuned security across all devices. Peace of mind has never been simpler.

ESET has always been in the business of protecting organisations from threats that prevent them reaching their potential. With ESET Endpoint Security for Android, you can be confident you’re protected and focus on the important parts of running a business.

Improved detection
Stronger security and better detection. Delivers real time on-access scanner with improved scanning speed, integrated ESET Live Grid, scheduled scanning, enhanced virus database updates and anti-phishing.

New and improved features
Antivirus, SMS and call filter, anti-theft, application control, essential device management settings, remote and local administration, and import/export of settings, anti-phishing.

Ease of use
Improved user experience. Easier to navigate and use. ESET Remote Administrator management console and ESET Endpoint Antivirus/ESET Endpoint Security client software deliver a recognizable look and feel.

New licensing system
Will fully support the new licensing model introduced with ESET Remote Administrator. New licensing framework integration simplifies the deployment and long-term usage of ESET security software. Customers are able to swap license information for a simple to remember email address with a custom password.
A new, terrifying weapon is in the hands of hackers - the ability to stop a toilet flush from working. We look at 2015’s silliest prophecies of gadget doom.

The ‘Internet of Things’ - connected devices such as lamps, fridges, cars or industrial equipment - has been the subject of much debate, and several rather over-the-top predictions from tech pundits. Will we all REALLY be killed by our fridges? We compile some of the deadliest, most murderous death machines ever to (theoretically) emerge from the Internet of Things.

Veteran security researcher and writer Graham Cluley feels unthreatened - and uninterested - by these connected devices. He is unconvinced that Hollywood will turn its hand to horror films based on murderous white goods - ‘Heartbreak Fridge’ perhaps.

“Yes, of course there are threats associated with more devices connecting to the Internet,” says Cluley. “Especially when they are built by companies who may not be well versed in computer security. Although none of us should be complacent about the potential risks, there is perhaps more hype than havoc at the moment.

‘1. for one, am not drooling at the thought of having an Internet fridge. Not because of the potential security risks, but simply because I can’t imagine how having an Internet-enabled fridge would make my life in any way happier or more convenient.”

The connected window blinds did it - a new way to kill?

Like many companies in the technology world, Rod Rasmussen peered into his crystal ball last year to predict likely events for 2014 - Rasmussen is the highly respected President and CTO of IID (Internet Identity). Rasmussen headed straight out for the territory where the buses don’t run - and predicted a murder using an Internet-connected device: “Killings can be carried out with a significantly lower chance of getting caught, much less convicted, and if human history shows us anything, if you can find a new way to kill, it will be eventually be used.” Being slammed in a toilet lid can sting - but is it really deadly? And will it finally happen in 2015?

Flushed to death?

At the Black Hat conference in Las Vegas, various terrifying hacks - such as the ability to peer through home security cameras - have been shown off, but it was the demonstration of an e-toilet hack which ran off with the headlines. Terrified victims of the hack against Satis toilets could be assaulted with a remote-controlled flush - or even a blast from the bidet. Hackers can also use the app to control the air-drying functions at will, “causing discomfort” As‘ Technica warned with tongue firmly in cheek.

Knock, knock, hue’s there?

Terrifying headlines greeted the news that it was possible to remote-control the Philips Hue lighting system due to flaws in its online control panel. What these reports failed to mention, of course, is that Hue is more akin to a lava lamp than a home lighting system, with colors that flicker to match films on TV, or just to create a nice warm glow. Gizmodo warned that they are “highly hackable”. Surely it’s easier simply to run outside and jingle their wind chimes to ruin the vibe?

White goods - black heart?

The scene in Ghostbusters where Sigourney Weaver opens her fridge to reveal a portal into a demonic underworld came true this year. Well, nearly. Reports of a fridge sending huge volumes of spam swept the Web’s more credulous regions - with some reports claiming that other businesses had been targeted by the rogue chiller cabinet - until someone pointed out a nearby Windows PC was the culprit. The fridge has since been cleared of all charges.

Should you be scared of your fridge?

By Rob Waugh, We Live Security contributor
WHEN WHITE GOODS GO BAD

Is the ‘Internet of Things’ really as big a threat as some doomsayers predict?

By David Harley, Senior Research Fellow, ESET

Targeting devices that aren’t PCs and therefore probably don’t have an explicit malware detection mechanism would reduce the likelihood of early detection of device-specific malware. Payloads that would take advantage of device-specific functionality would require significant research and development, but who, a few years ago, would have given much thought to the likelihood of malware targeting uranium enrichment centrifuges? However, the fact that eavesdropping, sabotage and other attacks are or may be possible in surprising contexts doesn’t mean that they likely. The Internet may have elements of the Wild West (and always did), but it hasn’t turned into a gigantic stage set from 1984, even if a laptop or television screen can sometimes behave like Big Brother’s telescreens. (That’s the 1984 Big Brother, not the TV unreality show.) Nor are we all now players in a universal game of Cluedo (or Clue as it’s known in the U.S.) where Professor Plum is likely to be bumped off by wifi-controlled sabotage of his pacemaker, Colonel Mustard and his library are bumped off by wifi-controlled sabotage of his colored Hue lighting system, researcher Nitesh Dharmi said, ‘In this age of malware and powerful botnets, it is vital that people’s homes be secure from vulnerabilities like these that can cause physical consequences.’

THE PREDICTIONS

1) Someone will be killed by a connected device this year

Killings can be carried out with a significantly lower chance of getting caught, much less convicted, and if human history shows us anything, if you can find a new way to kill, it will be eventually be used.” CID President Rod Rasmussen

2) Worldwide threats will increase

“We’re connecting more of our world every day through smart, IP-enabled devices. It is, unfortunately, too easy to imagine how these world-changing developments could go terribly wrong when attacked or corrupted by bad actors.” Cisco Senior VP Security Chris Young

3) Your family could burn to death - or face higher electricity bills

“The vulnerabilities found within the Belkin WeMo devices expose users to several potentially costly threats, from home fires with possible tragic consequences down to the simple waste of electricity,” wrote device security specialists IOActive.

4) Hackers could start a disco in your home

On revealing a security flaw in Philips multi-colored Hue lighting system, researcher Nitesh Dharjani said, ‘In this age of malware and powerful botnets, it is vital that people’s homes be secure from vulnerabilities like these that can cause physical consequences.”

5) Cybercriminals could steal your steaks

At CES this year, the BBC warned that Smart Fridges may pose a risk. “In the future, it might not just be your smartphone that leaks personal and private data, it might be your smart fridge too,” the broadcaster warned. Steaks may tempt burglars to enter your home in search of dinner.

Making business more of a pleasure

ESET Endpoint Security and ESET Endpoint Antivirus: effective, light footprint security for your small to medium sized business

Businesses, no matter what their size, need I.T. security they can trust. Security systems that are easy to use, intuitive and do the job quietly and efficiently, while requiring as little attention as possible. With ESET Endpoint Security and ESET Endpoint Antivirus, ESET has met these goals, making it the ideal solution for small to medium sized businesses.

Widely regarded in the business and technology community as one of the best systems against cyber threats around, ESET Endpoint Security calmly and efficiently eliminates current known threats, but also keeps an eye on the future. With new viruses and malware being created every day, ESET Endpoint Security doesn’t simply wait for new definitions to be downloaded – it proactively looks out for suspicious activity, and lets the user know when it spots something that’s likely to be currently undefined malware.

Offering improved detection, anti-phishing, an advanced memory cleaner, an exploit blocker, and a firewall, among other methods of protection, the software protects on a variety of levels, against myriad threats, while maintaining a small footprint. For the first time, ESET offers dedicated botnet protection, which helps to uncover undiscovered malware by analyzing network communication patterns and protocols, along with the usual expected quality virus and malware detection, and protection from suspicious URL and file-types.

For the administrator, it’s easy to set up and maintain, ensuring that the entire network is protected by ESET’s advanced I.T. security, while less tech-savvy employees will find the protection subtle and non-invasive, allowing them to work without unnecessary distractions.

To find out more about ESET’s security solutions for organizations of all sizes, visit: www.eset.com/int/business/solutions

ESET Endpoint Security and ESET Endpoint Antivirus: effective, light footprint security for your small to medium sized business
With the new ESET Remote Administrator, ESET seeks to address the real-life issues facing security administrators in small companies. It abandons the old, endpoint-server architecture in favor of a more modern, progressive server-agent approach.

ESET Remote Administrator comes shipped as a platform-independent product (now available on Linux-based systems), allowing seamless integration with customers’ virtual infrastructure.

The new version of ESET Remote Administrator will be the central hub for all existing and upcoming ESET business products, able to manage all ESET products centrally.

In addition to this, the Web-based administration console offers the ability to connect from almost any location or device, making administration effortless.

**STAY SECURE: WHEREVER YOU ARE**

ESET Remote Administrator keeps you on top of your corporate security, whether you’re in the office or on the other side of the world.

**BENEFITS**

- **Ease of deployment**
  Migration wizard for existing ESET customers and one-step installation for new users.

- **Multi-platform support**
  ESET Remote Administrator runs on both Windows and Linux machines, cutting costs for cross-platform users.

- **New user experience**
  A reworked console makes Remote Administrator simple to navigate and accessible from anywhere via your browser.

- **Performance**
  ESET Remote Administrator can handle even the largest computing networks from a single centralized server.

- **New architecture**
  Tailored towards the needs of individual customers, from basic setups to complex multi-user scenarios.

- **New licensing system**
  Simplified licensing with a new license key format and automatic updates means you’re always protected.

**BEST FOR...**

- **Small to medium-sized businesses**
  With fewer resources to dedicate to infrastructure security, small to medium-sized businesses will find the combination of ease of use, value, and minimal impact on systems of ESET Remote Administrator appealing.

- **Security conscious business consumers**
  ESET’s reputation in the field is second to none. Those looking for a reliable, proven, customizable, small footprint solution need look no further.
Fact: Many such attacks are transient but digital data is actually extraordinarily persistent.

Given these issues, it is worth considering if it’s a parent’s ethical – or even moral – responsibility to think about the difference between the online and offline contexts and act accordingly.

There are clearly lines to be drawn, of course, between digital data which can be damaging, and that which cannot.

My own daughter’s reaction to the publishing of photos was this: “Ultrasounds, baby photos, etc, I think could be considered acceptable – at the end of the day a child is a child. The photos do not have the same long-term problems as, for example, employers getting to see embarrassing teenage photos, posted by parents, or, more likely, friends.”

Fact: Antivirus software is dead

Fact: The way security software detects malware has changed

Fiction: Antivirus failed to stop the Target breach

Fiction: Antivirus is dead

We’ve seen this announced so many times we’ve taken to carrying black ties. Actually, anti-malware technology moved on long ago, but customer and media perception has lagged way behind. Much malware – spear-phishing, APT – is now highly targeted, meaning that no I.T. security company will claim 100% malware detection. But this just means it’s changed. Current malware detection comes in three main forms:

Proactive detection and blocking

The holy grail of security: proactive blocking through reputational and generic countermeasures.

Detection of known malware

A high proportion of threats continue to be detected either specifically or using more generic detections.

Remediation

These days, anti-malware and protection is achieved through reputation and behavior analysis, and with the aid of advanced heuristics, while signatures are primarily used for remediation where proactive methods have failed. Don’t be too optimistic about finding a single solution. The best advice is to look for a combined solution that you can afford.

Fact: Blackberry is dead

Fiction: It was detected daily – staff failed to notice

Let’s examine some of the myths about the Target breach:

(1) The person who created the malware perpetrated the breach.

Knowing who created the malware doesn’t tell us who carried out the attack – it is only one tool that the attacker or attackers used.

(2) The code was not detected in VirusTotal, so antivirus failed.

The idea that VirusTotal can be used as an accurate test of whether up-to-date antivirus software would detect malware has been debunked.

(3) The attackers must be geniuses.

Malware authors are not geniuses – they are simply resourceful about combining information that’s widely available.

(4) There’s no way to stop such attacks.

The usual security advice should have been followed. It wouldn’t. Attackers only hit big businesses.

Attacking a big business is certainly a huge payday – but lots of little attacks can quickly match it. High-profile breaches like this should remind businesses that it’s worth the expense to improve their security.
ESET ENDPOINT SECURITY FOR ANDROID

Do More with your Android endpoints secured

- Secure your company smartphones and tablets, wherever business takes them.
- Protect all applications, files and memory cards.
- Track phones that go missing and lock them remotely.

ESET ENDPOINT SECURITY

WWW.ESET.COM

8 tips to protect your business

By Carole Theriault, Director, Tick Tock Social

We all know that having employees trained in safe computing practices is a good idea. Not only does it help to protect the integrity of the network, but having alert and informed users can provide an extra layer of security as they can raise the alarm if they see something suspicious.

The problem many companies face is how to get users on board. Some companies use fear tactics, threatening reprimands and even dismissal if users are found to have breached protocol. Having IT teams act like office authorities may seem like a good idea, but it does have a serious downside: a user who screws up or sees something suspicious may shy away from reporting the problem to avoid the consequences.

There is a better approach. It does take some resources to set up, but running an internal security campaign that informs and encourages users about the key security points helps to safeguard your own network, and it will also provide them with skills they can use at home to keep their own computers free from malicious attacks.

With that in mind, we’ve created eight security tips for you to share with your employees.

Security tips

Security breaches are no fun for anyone, and are best avoided at all costs. While you will have security in place to protect the network, you’ll need employee help to keep risks to a minimum and alert you if they see something suspicious. Check out these tips to help you prevent any of the bad stuff from getting in:

1) Keep sensitive information out of sight.
When you have visitors in the office, keep all sensitive information out of sight. Avoid leaving any information lying around, on your desk, shared meetings rooms and at the printer or photocopier.

2) Lock your devices.
Set your computer, laptop, tablets and mobiles to lock automatically after two minutes of non-activity, keeping them safe from prying eyes.

3) Think before you share information on the phone.
Avoid giving away employee, financial or sensitive company information on the phone. Try to verify the caller’s identity. And if something like this doesn’t feel right, report it to your boss or the IT team.

4) Consider using an application to manage passwords.
Having strong, unique passwords for each login is important, but impossible for users to remember. Use a password manager – then you only need to remember one password. Remember to make your master password strong.

5) Watch out for suspicious emails and dodgy links.
Suspicious emails and links should not be opened or even previewed. Just delete them. Opening or viewing these emails and links can compromise your computer and invite in an unwanted problem.

6) Tell IT before you connect personal devices to the network.
Devices like USBs, music players and smartphones can be compromised with code waiting to launch as soon as they are plugged into a computer. Talk to IT and let them make the call to keep you and your company safe.

7) Don’t install unauthorized apps or programs on your work devices.
Check with IT before installing unauthorized programs on your company devices. Malicious applications often pose as legitimate programs, like a game, a tool, and even security software!

8) Avoid using an unprotected network.
When you travel, you might be tempted by free Wi-Fi. The issue is that these networks can be compromised. Make sure you talk to IT before you connect, so they can provide you with a VPN to make your connections more secure.

1) Keep sensitive information out of sight.
When you have visitors in the office, keep all sensitive information out of sight. Avoid leaving any information lying around, on your desk, shared meetings rooms and at the printer or photocopier.

2) Lock your devices.
Set your computer, laptop, tablets and mobiles to lock automatically after two minutes of non-activity, keeping them safe from prying eyes.

3) Think before you share information on the phone.
Avoid giving away employee, financial or sensitive company information on the phone. Try to verify the caller’s identity. And if something like this doesn’t feel right, report it to your boss or the IT team.

4) Consider using an application to manage passwords.
Having strong, unique passwords for each login is important, but impossible for users to remember. Use a password manager – then you only need to remember one password. Remember to make your master password strong.

5) Watch out for suspicious emails and dodgy links.
Suspicious emails and links should not be opened or even previewed. Just delete them. Opening or viewing these emails and links can compromise your computer and invite in an unwanted problem.

6) Tell IT before you connect personal devices to the network.
Devices like USBs, music players and smartphones can be compromised with code waiting to launch as soon as they are plugged into a computer. Talk to IT and let them make the call to keep you and your company safe.

7) Don’t install unauthorized apps or programs on your work devices.
Check with IT before installing unauthorized programs on your company devices. Malicious applications often pose as legitimate programs, like a game, a tool, and even security software!

8) Avoid using an unprotected network.
When you travel, you might be tempted by free Wi-Fi. The issue is that these networks can be compromised. Make sure you talk to IT before you connect, so they can provide you with a VPN to make your connections more secure.
A SCAM-SPOTTER’S GUIDE: THINGS YOUR BANK WILL NEVER DO – BUT CYBERCRIMINALS WILL

By Rob Waugh, We Live Security contributor

Technologies change, but cybercriminals will always dream up new ways to fool you into handing over your bank details, whether via phishing emails, SMS or phone.

These days cybercriminals will use phone calls and even couriers in an effort to get your money. Many of these attacks can seem very convincing. The key to staying safe is to recognize behavior that isn’t quite ‘right’. Here are some things a bank will never do – but a phisher, or thief, will.

**Text asking for details to “confirm” it’s you**

Your bank will never text you, for instance to confirm an online transaction, but bank texts will not, ever, ask you to confirm details such as passwords. Banks also won’t update their apps in this way – their websites may be blocked. If your bank account erases itself or vanishes, you are looking at a scam.

**Don’t ever click a shortened link.**

Use shortened URLs in an email.

Cybercriminals use a variety of tricks to make a malicious Web page appear more “real” in an email that’s supposedly from your bank – one of the most basic is URL-shortening services. Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a message with a blank address field**

Use an unsecured Web page.

If you’re on a ‘real’ online banking page, it should display a symbol in your browser’s address bar to show it is secure, such as a locked padlock or unbroken key symbol. If that symbol’s missing, be very, very wary. This is one reason why it’s best to browse an online banking page from your computer – on a smartphone, it can be more difficult to see which pages are secure.

**Send a courier to pick up a “faulty” card**

Address you as “Dear customer” or dear “youremail@gmail.com”

Banks will usually address you with your name and title – i.e. Mr Smith, and often add another layer of security such as quoting the last four digits of your account number, to reassure you it’s a real email, and not phish. Any emails addressed to “Dear customer” or “Dear [email address]” should be treated as spam.

**Email you at a new address without asking for a new way to get in touch**

Send a message with a blank address field.

If you receive a personal message from your bank, it should be addressed to you – not just in the message, but in the email header. Check that it’s addressed to your email address – if it’s blank, or addressed to ‘Customer List’ or similar, be suspicious.

**Call your landline and “prove” it’s the bank by asking you to call back**

Ask for your mother’s maiden name

A common new scam is a phone call from either ‘the police’ or ‘your bank’, saying that fraudulent transactions have been detected on your card. The criminals will then ‘prove’ their identity by “hanging up” and asking you to dial the real bank number – but they’ve actually just played a dial tone, and when you dial in, you’re talking to the same gang member, who has remained on the phone, waiting, and who will then ask for credit card details and passwords.

**Email asking for details to “confirm” it’s you**

Send a message with a blank address field.

If your bank suddenly contacts you on your work email (or any other address than the one they usually use), worry. Banks will not add new email addresses on their own. If you want to be ultra-secure, create a special email address just for your bank, don’t publish it anywhere, or use it for anything else – that way, emails that appear to be from your bank probably ARE.

**Use an unsecured Web page**

Address you as “Dear customer” or dear “youremail@gmail.com”

Banks will usually address you with your name and title – i.e. Mr Smith, and often add another layer of security such as quoting the last four digits of your account number, to reassure you it’s a real email, and not phish. Any emails addressed to “Dear customer” or “Dear [email address]” should be treated as spam.

**Send a message with a blank address field**

Send a message with a blank address field.

If you receive a personal message from your bank, it should be addressed to you – not just in the message, but in the email header. Check that it’s addressed to your email address – if it’s blank, or addressed to ‘Customer List’ or similar, be suspicious.

**Call your landline and “prove” it’s the bank by asking you to call back**

A common new scam is a phone call from either ‘the police’ or ‘your bank’, saying that fraudulent transactions have been detected on your card. The criminals will then ‘prove’ their identity by “hanging up” and asking you to dial the real bank number – but they’ve actually just played a dial tone, and when you dial in, you’re talking to the same gang member, who has remained on the phone, waiting, and who will then ask for credit card details and passwords.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.

**Email asking for details to “confirm” it’s you**

Don’t ever click a shortened link. Go to the bank’s Website instead (the usual URL you use), or call them.

**Send a courier to pick up a “faulty” card**

The courier scam is a new one – your phone rings, it’s your bank, and they need to replace a faulty bank card. The bank tells you that a courier will arrive shortly. A courier turns up, asks for your PIN as “confirmation”, and your money vanishes. If your card is faulty, a real bank will instruct you to destroy it.
Cybercriminals always look for the weakest link when planning their attacks – often it’s human error, such as weak passwords or opening phishing emails, but failings in home routers can allow another ‘way in’.

Over the past year, researchers have repeatedly shown that the devices can contain “backdoors” which allow attackers access to your private data. Once known, this information will circulate rapidly among cyber gangs. We also don’t help ourselves. A study of 653 IT and security professionals and 1,009 remote workers found that 30% of IT professionals and 46% of remote workers do not change default passwords on their routers. So far, router attacks are a new and evolving phenomenon – but it’s worth protecting yours.

1) Don’t leave your username as ‘admin’
The first, and most important step, is to change your router’s password from its default. Routers ship with a Web page allowing users to adjust settings, with default passwords and usernames such as “admin”. These are widely known to hackers, and should be changed immediately.

2) For extra security, change the firmware
A recent survey found that around 80% of the top-selling “small office/home” routers on Amazon shipped with known “critical” vulnerabilities, making them easy prey for cybercriminals. ESET Malware Researcher Olivier Bilodeau says, “For the relatively advanced consumer: install an alternative open source firmware on your router.” These are replacement versions of the official firmware – and often more secure. This is not for beginner PC users, but clear instructions can be found online as to how to install. Bilodeau recommends:
- Tomato: www.polarcloud.com/tomato
- DD-WRT: www.dd-wrt.com/site/index
- Open-WRT: https://openwrt.org/

3) Make sure your encryption is up to scratch
Older routers with WEP encryption are vulnerable – check which one you’re using on your settings page. If it’s WEP, change to the more secure option WPA. Or buy a new router.

4) Don’t tell the neighbors your name
Wi-Fi networks have a network name – known as an SSID – and most ship with a default name, which often includes the brand. For a potential attacker – for instance, against a small business – this is useful information. Some models have vulnerabilities that make router attacks easy. It’s worth considering making yours a “hidden network” – disabling the broadcast of the SSID’s name. That way you’re less visible to attackers – and to connect new devices, simply type in your network’s name on the gadget.

5) Know who’s connecting to your network
Any PC or mobile computing device has a unique identifying number known as a MAC address. If you access your router’s settings, you can select which devices can and cannot connect to your network – meaning for instance, a neighbour couldn’t log in, or a teenager visitor could not access unsuitable sites via a smartphone. Add the MAC addresses of all authorized devices in the home – iPhones, tablets, laptops etc. – to the router’s authorized list. No other device will then be allowed. You can find the MAC addresses of mobile phones and other portable devices under their network settings, though this will vary for each device. Check with the manufacturer.

Around a third of IT professionals admit to never changing the default settings on routers, giving cybercriminals a potential ‘way in’ to networks.
Small fish, big risks

Why even the smallest businesses need to have a security policy in place.

By Stephen Cobb, Senior Security Researcher, ESET

A while back, I offered a Webinar on information security policy entitled “How can your small business make security policies pay off?” If you missed it, there’s a recording at eset.com that you can view at any time.

During the question-and-answer session towards the end of the recording, a member of the audience asked the following: “You talk about policy singular but also multiple policies. Which do I need?”

This really got me thinking about how information security people talk about policy and I realized it can be confusing. So here are some explanations about security policy, policies, and a thing called WISP.

First of all, what does it mean for an organization to have an information security policy? Singular? It means that the organization has stated and recorded its commitment to protecting the information that it handles.

For example, here’s what Acme Bicycle Company might say: “It’s the policy of ABC Company that, as defined hereinafter, in all its forms—written, spoken, recorded electronically or printed — will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit information.”

This statement of overall policy usually appears as the preamble to a series of more specific policies. For example, there may be a section on risk management:

“A thorough analysis of all ABC information networks and systems will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information.”

There should probably be a virus protection policy. That might say something like this:

“Virus-checking systems approved by the Information Security Officer and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus-checking systems.”

So there are multiple specific policies below the overall information security policy. There is another term you may see when people talk about information security policy and that is Information Security Program, and sometimes written information security program or WISP (not to be confused with wireless Internet service provider). WISP is a term that encompasses all relevant policies plus your organization’s program for implementing them. I like the term because it implies something more practical than just a collection of policies sitting in a binder (although the WISP will likely sit in a binder, too). Regular readers may recall that WISP plays a prominent role in some information security legislation, notably the law in Massachusetts that says:

“Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards...”

I won’t go into the details about the Massachusetts legislation since the main points were covered in that earlier article, but suffice it to say I think that every business, large or small, needs to have a WISP. This may simply be an attachment to existing policies that says:

“The ABC Written Information Security Program consists of the enclosed policies and the steps we take to enforce them, including dissemination of policies to all new employees and the regular training of all employees on how to uphold the policies in their work, together with a periodic management review of the program to ensure that all aspects of information security in our organization are appropriately addressed at all times.”

Now, if you meet resistance when it comes to the not inconsiderable effort of creating and executing a WISP, try persuading skeptics with a litany of examples of genuine small firms that went out of business or suffered severe losses because of cyber criminals, many of whom could have been defeated if the victim had been on top of the problem.

Where to find the facts? The highly reliable Brian Krebs has a sobering collection of small biz cases, constantly updated.

Why a WISP may deal you a winning hand

Suppose you run the Acme Bicycle Company and have developed a new style of bicycle pedal. Will Joe Consumer, who just wandered into your retail store, ask to see your WISP before he buys pedals from you? Probably not. But suppose you’re bidding to supply a lot of pedals wholesale to the MegaSports chain. Will MegaSports want to see your WISP? Probably.

I have seen the lengthy compliance documents that some large companies present to smaller ones with whom they want to do business, and without a WISP, it is going to be hard to comply in a timely fashion, which means you could lose the business to a competitor who already has its security program in place and documented. Here is language from one such document which was attached to a juicy contract, as a condition of doing business:

“Vendor must have a written policy that addresses information security, states management commitment to security, and defines the approach to managing information security.”

And here are some questions which another big vendor put to an SMB, again as part of the contract process:

Are there documented policies and procedures for managing security?

Does the vendor perform internal reviews of security policy and technical compliance?

Are security policies and procedures disseminated to all vendor employees?

So, getting your information security policy in order is not a wish-list item or a “nice to have but not essential” extra for your business. Not only is a WISP essential to succeed in fending off the bad guys (who are most definitely targeting small businesses these days), it also helps you to win business.

You could lose business to a competitor who has a security program in place.
The big mistakes YOUR company could be making with passwords

Enforce a password policy that requires regular, substantial changes. It is common to simply add numbers or special characters on the end. These customized passwords are a gift for criminals to crack.

Don’t trust your employees to abide by policies. A password-strength meter on the password entry page will help employees understand why some passwords are better, and how to choose a secure one.

The programs criminals use will also look for parts of employees’ names or usernames being reused in your password.

The programs criminals use will also look for parts of employees’ names or usernames being reused in your password.

Much in the same way that Heisenberg has become a popular name for babies in the wake of the TV series Breaking Bad, popular films and books are a common password choice – and this weak.

If your site is breached, change EVERY password. Eventually, left unchanged, even strong passwords WILL crack.

The password pill

Regina Dugan of Motorola showed off a password you can actually eat – a vitamin-style pill that dissolves in stomach acid, and can be read by scanners to authenticate the wearer.

“I take vitamins every day, why can’t I take a vitamin authentication every day?” asked Dugan. “Your entire body becomes an authentication token. It becomes your first superpower: when I touch my phone, computer, front door, or car I am authenticated.”

The brainwave-scanning hat

Wearing an electronics-laced hat as a car key might seem surreal but according to researchers at Tottori University, the device could provide near-unbreakable security. “Measuring the driver’s brainwaves continually would be straightforward and allow authentication that could not be spoofed by an imposter,” the researchers write. “If the wrong brainwaves are detected, the vehicle is immobilized.”

The brainwave-scanning hat

Wearing an electronics-laced hat as a car key might seem surreal but according to researchers at Tottori University, the device could provide near-unbreakable security. “Measuring the driver’s brainwaves continually would be straightforward and allow authentication that could not be spoofed by an imposter,” the researchers write. “If the wrong brainwaves are detected, the vehicle is immobilized.”

The tongue scanner

Tongueprints are not about to replace fingerprints – but Google may soon require us to waggle our tongues at the camera for its face passwords. A long-standing problem with any visual password system is that some can be fooled by photographs – hence Google patented a facial-password system, where users could unlock phones using facial expressions. So you’d have to stick out your tongue or frown at the camera instead of typing a password.

The passwordocracker app Hashcat can now deal with. Previously, security wisdom was “the longer the better” – but even long passwords are no longer immune.

The passwordocracker app Hashcat can now deal with. Previously, security wisdom was “the longer the better” – but even long passwords are no longer immune.

Regina Dugan of Motorola showed off a password you can actually eat – a vitamin-style pill that dissolves in stomach acid, and can be read by scanners to authenticate the wearer.

“I take vitamins every day, why can’t I take a vitamin authentication every day?” asked Dugan. “Your entire body becomes an authentication token. It becomes your first superpower: when I touch my phone, computer, front door, or car I am authenticated.”

The brainwave-scanning hat

Wearing an electronics-laced hat as a car key might seem surreal but according to researchers at Tottori University, the device could provide near-unbreakable security. “Measuring the driver’s brainwaves continually would be straightforward and allow authentication that could not be spoofed by an imposter,” the researchers write. “If the wrong brainwaves are detected, the vehicle is immobilized.”

The tongue scanner

Tongueprints are not about to replace fingerprints – but Google may soon require us to waggle our tongues at the camera for its face passwords. A long-standing problem with any visual password system is that some can be fooled by photographs – hence Google patented a facial-password system, where users could unlock phones using facial expressions. So you’d have to stick out your tongue or frown at the camera instead of typing a password.

The passwordocracker app Hashcat can now deal with. Previously, security wisdom was “the longer the better” – but even long passwords are no longer immune.

The passwordocracker app Hashcat can now deal with. Previously, security wisdom was “the longer the better” – but even long passwords are no longer immune.

Regina Dugan of Motorola showed off a password you can actually eat – a vitamin-style pill that dissolves in stomach acid, and can be read by scanners to authenticate the wearer.

“I take vitamins every day, why can’t I take a vitamin authentication every day?” asked Dugan. “Your entire body becomes an authentication token. It becomes your first superpower: when I touch my phone, computer, front door, or car I am authenticated.”

The brainwave-scanning hat

Wearing an electronics-laced hat as a car key might seem surreal but according to researchers at Tottori University, the device could provide near-unbreakable security. “Measuring the driver’s brainwaves continually would be straightforward and allow authentication that could not be spoofed by an imposter,” the researchers write. “If the wrong brainwaves are detected, the vehicle is immobilized.”

The tongue scanner

Tongueprints are not about to replace fingerprints – but Google may soon require us to waggle our tongues at the camera for its face passwords. A long-standing problem with any visual password system is that some can be fooled by photographs – hence Google patented a facial-password system, where users could unlock phones using facial expressions. So you’d have to stick out your tongue or frown at the camera instead of typing a password.

The passwordocracker app Hashcat can now deal with. Previously, security wisdom was “the longer the better” – but even long passwords are no longer immune.
Love your Android

Why malware protection is just the start for effective security on Android smart devices

By Branislav Orlik, Product Manager, ESET

Android devices face a wide range of dangers - from a colleague reading your emails over your shoulder (surprisingly easy, and something which no app can defend against) to more serious threats - from theft to phishing sites.

ESET Mobile Security aims to provide peace of mind. It is not built around scare tactics - used by some companies - where the threat of high-tech new malware is hyped at every opportunity. It’s built to allow users more control, and to deal with every problem the user faces while browsing or using apps, not just the ones that make good headlines on the tech blogs. ESET Mobile Security provides protection even for less experienced users. Our app is a new way of thinking about Android security - and a new level of peace of mind for our users.

Android under attack

Malware on devices using Android OS is a growing problem. ESET’s Virus Radar detects new variants of malware daily - including serious threats such as ransomware - and the malware itself is becoming more dangerous month by month. But the sheer number of Android devices brings a new set of security concerns apart from malware. Our app focuses on protecting your data 24/7 - however users use their handsets. We wanted to ensure users were protected in every eventuality.

Some Android users take big risks - using third-party unofficial stores or downloading cracked apps from stores outside official Google’s Play store. ESET Mobile Security will provide clear warnings to users, even for those. Moreover, Google itself has improved security in the Google Play store, and we have ensured that Mobile Security provides added value on top of that.

What’s the real problem?

Serious security vulnerabilities are patched rapidly - and consumers are often safe before the vulnerability is known to the public. The open nature of Android means that malware and various vulnerabilities will always be around - but for many users, these are not the real problems. ESET Mobile Security app protects the users first. Their devices contain personal details - for gangs, it’s not worth breaching, in the same way as they might hack a major company, so criminals use malware to “leech” instead. Leeching personal information is not the only threat, either - malware can cost you money - some malicious Android apps can bypass the “two-factor” security systems used by online banks, allowing criminals access to user’s accounts, or can send premium SMS messages or make calls to expensive numbers.

What ordinary users worry about

For an ordinary Android user, the biggest problem is “data leeches”. When a user installs an app, they will see a list of permissions - such as making calls, sending SMS messages or even for recording video without the user’s knowledge (as happened recently with Facebook’s Messenger). It’s easy for apps to misuse this data - particularly when adware harvests information without permission, and it is sold to third-party data brokers - or when apps fill your devices with full-screen ads. Users also face simpler problems, such as when a thief snatches a handset and sells identifying information. ESET Mobile Security blocks all of these threats - from rogue apps, to human thieves, to phishing sites. In their review, AV-Comparatives described our app as “outstanding”.

How IT security is changing

The way users interact with their devices has changed hugely. Anti-virus packages are an old way of doing things. For a user, their family photographs and contacts list are important - hence ESET Mobile Security doesn’t restrict itself simply to chasing high-profile malware. It also protects against theft or loss - allowing a remote wipe, siren, or geo-location of a lost handset. ESET Mobile Security will help to not only recover it. This is the modern face of phone security software.

Home users and ‘BYOD’

Android malware can threaten the privacy of anyone - private users, or big companies. Much of the malware infecting the world’s army of Android handsets is built to insert aggressive adverts throughout the OS - or to obtain identifying information.

The trend for users to ‘bring their own device’ to work can undermine corporate security, unless employees use an app such as ESET Mobile Security, which will help to underline the security rules of the company, when used in partnership with IT staff. For example, at last year’s I/O conference, Google announced a billion active Android users. Most of these users will try ‘freemium’ apps, offered in millions, which can harvest data on a scale never seen before.

What does ESET Mobile Security offer its users?

ESET Mobile Security gives users significant control over devices that increasingly contain information more valuable than the phones themselves. It is easy to install, the database of threats is updated daily - and the app walks users through all of its functions. Avoid of what has happened to your lost device? Remote-wipe it. Worried that your app has too many permissions? We will warn you. And our Live Grid and regular scans ensure that if a ‘big’ Android malware attack hits, our users are ready.

Scammers, thieves, phishers, and malware writers will have a much more difficult job if your device runs the ESET Mobile Security app - constantly updating to ensure we’re always a step ahead.
Why do so few kids learn computer science?

Lysa Myers, Security Researcher, ESET

The city of Chicago, Illinois recently announced a change to the curriculum for schools in their district that would introduce children as young as primary school age to computer science concepts. It would also allow students to count computer science as a core subject that fulfills graduation requirements, rather than simply be an elective.

This sounds like a big step in the right direction. But what does the boost for computer science, often affectionately abbreviated to comp-sci, mean in the grand scheme of things?

Why does K-12 computer science matter?

For those of us who have been out of high school for more than a few years, this announcement from Chicago might come as a surprise. Aren’t all kids getting computer science classes already?

The percentage of people needing to use computers proficiently seems to be rapidly approaching 100%, at least for skilled jobs in the US. And in terms of job security and satisfaction, technical jobs have much to offer. In lists of the best, the most lucrative and most in-demand jobs, computer experts are always in the top five.

One might think that getting kids interested in computers would be considered something of the utmost importance. But apparently this is not yet the case. In many states in the US, if computer science is offered at all, it is considered an elective subject, which means it does not count towards a student’s graduation requirements.

What is happening elsewhere?

I naturally wondered how this compared with that of other countries. The US is behind some countries, ahead of others, but few are perfect.

To get an idea of the differences in culture, let’s look at a couple of very dissimilar examples. In Finland, which is generally the country in Europe whose scores in reading, math and science are consistently highest, there is little focus on taking standardized tests. Being strong in multiple languages is a primary focus for their educational system.

In South Korea, another very highly-rated country, things are very different. Students typically go to school for incredibly long hours. In both Korea and Finland, like in the US, computer science is considered an elective. But in practice, Korean students get much more exposure to computer-related topics, in part because those long days give them more time. There is also much more focus on digital literacy and ethics.

But digital literacy is not the same as understanding how computers actually work. Computer Science in many countries may cover no more than basic Java programming. For those of us in a computer-related field, this is laughably inadequate. But fortunately, there are things that you and I can do.

Ask your local teacher about computer education

Does your local school teach children how to use computers safely? What other subjects do they cover, such as programming or algorithms?

Sign a petition to make computer science count. For the US, there are already several on Change.org.

Learn more at Code.org

Code.org has an incredible variety of resources available for people that want to help spread the word.

For those who are educators, or who have kids they would like to inspire, they have even more options to offer. If you are a software engineer, they include yet another list of ways you can help. And last but not least, donations are always helpful.
Whether you’re managing your business, or overseeing your company’s I.T., ESET’s security products are fast, easy to use, and deliver market-leading detection. We deliver the protection that allows you to DO MORE. Find out more at ESET.COM.