



SECURITY is not complete without **U**

Some simple tips to protect your computer and data

CERN Articles on Computer Security

Full list available at: <http://cern.ch/go/6kCF>

By **CERN Computer Security Team**,

<http://cern.ch/security>

19 May 2014

V1.0

Publication prepared by the CERN IT Department



This publication is released under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/).

Front image credit: CERN

Table of Contents

Computer Security	5
Public PCs: Log Out or Lose Out.....	5
Don't put your family at risk.....	5
Got a call from "Microsoft"? The social way infecting your PC.....	5
Infesting Windows, Linux & Mac in one go	5
Gotcha! Macs lose their innocence	5
Found a USB stick? Go and infect your PC!	6
Why I like power cuts... ..	6
25 years - Happy Birthday!	6
Bye, Bye, Windows XP security... Welcome infections!	6
Network Security	7
After Prism & Tempora: How much monitoring is OK for CERN?.....	7
The Lure of Wireless Encryption	7
Encryption is Useless!?	7
Email & Web Security	8
Jekyll or Hyde? Better browse securely.....	8
Browsing the Internet: good-bye anonymity!	8
Don't let your mail leak.....	8
Don't screw up your web.....	8
You've received a Hallmark E-Card? Delete it!	9
Cloud Security.....	10
Prison or "Prism"? Your data in custody.....	10
When the "Lion" eats your data	10
Send your data into the cloud and make it... vaporize	10
Mobile Security.....	11
Backed up and gone.....	11
BYOD: Bring your own disaster.....	11
Android is the new Windows.....	11
... and thank you for your mobile data!	11
One photo to rule your phone.....	11
Smartphone lost - Privacy gone	12

Is your Android running a temperature?.....	12
iphones, Androids, and history repeating	12
Passwords	13
No certificate, no chocolate.....	13
Don't let Chrome expose your passwords.....	13
Maths to the rescue!	13
Creativity@CERN	13
Train your brain: Don't put your password on paper!.....	13
1000 passwords exposed, what about yours?.....	14
Holidays Come - Passwords Go.....	14
What is a good Toothbrush, erm, Password?.....	14
What do passwords and toothbrushes have in common?	14
When a person leaves - access rights remain!	14
Copyrights	16
Getting a better image from the Organization.....	16
Bad (Re)Presentations	16
Software licenses: Stay honest!	16
Music, videos and the risk for CERN	16
Data Protection.....	17
How private is "private"?.....	17
Let's play hide and seek!.....	17
Your privacy is paramount!.....	17
"Clas-si-fied (/ˈklæsɪfaɪd/)" - What's that?	17
Data Protection for All	18
How to get properly rid of confidential data?	18
Classified	18
Privacy, who cares?.....	18
Coming soon, a pragmatic Data Protection Policy for an open Organisation	18
Easy encryption for CERN laptops	19
Policies	20
CERN: Digitally open, too	20
Don't tempt me!	20
The Naked Blunder	20
Why "Security" is not ME.....	20

“Security” is YOU!	20
Social Media - Dos and Don'ts	21
Secure Coding	22
Stop fighting alone, let synergy rule!.....	22
Why can't I sue my software provider?	22
A Short Tale of the Black Sheep of –ITY	22
Raise your defence: a baseline for security	22
... An example of flawed code	23
Do you write secure code?	23
Improve software, avoid blunder	23
Risk Management	24
Cyber-Attacks and the Risks for CERN	24
Hacking control systems, switching... accelerators off?	24
Hacking control systems, switching lights off!.....	24
Miscellaneous	25
Security bingo for administrators	25
Security bingo for the paranoid	25
Security Bingo	25

Computer Security

Public PCs: Log Out or Lose Out

Do you regularly use one of the public Windows or Linux terminals in the CERN library or in front of the Users' Office? Or do you often give presentations or run meetings, workshops or conferences? Did you recently attend a training session in the CERN Training Centre? If you answered at least once with "yes", we have a plea for you: LOG OUT when done in order to protect your data!

Read the full article at: <http://cds.cern.ch/record/1615057?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1615057?ln=fr>

Don't put your family at risk

How easy is it to fall into the trap of cyber-criminals? Get one's online banking password stolen? Lose photos to third parties? It's easier than you think. One single click to open a malicious attachment or a malicious web page is sufficient to put your family at risk.

Read the full article at: <http://cds.cern.ch/record/1527119?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1527119?ln=fr>

Got a call from "Microsoft"? The social way infecting your PC

Have you recently been called by "Microsoft Security"? At home!? Then beware: these are fake calls trying to make you install malicious software on your (home) PC!

Read the full article at: <http://cds.cern.ch/record/1479370?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1479370?ln=fr>

Infecting Windows, Linux & Mac in one go

Still love bashing on Windows as you believe it is an insecure operating system? Hold on a second! Just recently, a vulnerability has been published for Java 7.

Read the full article at: <http://cds.cern.ch/record/1475394?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1475394?ln=fr>

Gotcha! Macs lose their innocence

Still believe your Mac is secure because Microsoft PCs fall prey to viruses and worms but Macs don't? Time to wake up! This year has seen the first major compromise of Macs worldwide*. How is yours doing?

Read the full article at: <http://cds.cern.ch/record/1443480?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1443480?ln=fr>

Found a USB stick? Go and infect your PC!

Err. Wait. Please no! USB sticks are not innocent little things. They can quickly mutate into malicious nasty beasts! Just in the recent past, at least two physics experiments were suffering as their control and data acquisition PCs, respectively, were infected by USB sticks holding malicious code. A bit longer ago, a series of laptops were infected at a 2008 computing conference as an infected USB stick made its tour around. Bad luck for those who ran a Windows operating system and inserted that stick...

*Read the full article at: <http://cds.cern.ch/record/1424411?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1424411?ln=fr>*

Why I like power cuts...

Accidental power cuts - a permanent nuisance when running accelerators or computing services, since it takes a lot of time to recover from them. While I feel very sorry for those who are under pressure to get their service running again and deeply regret the loss of down-time and availability, I must admit that I like power cuts: power cuts make computers reboot! And rebooting computers at CERN means all the pending software patches are automatically applied.

*Read the full article at: <http://cds.cern.ch/record/1417210?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1417210?ln=fr>*

25 years - Happy Birthday!

The nasty PC virus turned twenty-five years this month. The very first computer virus ever was created in January 1986. Dubbed "©Brain", this virus was aiming to infect DOS-based PCs. While this instance was relatively harmless and their creators claim sincere intentions, the world has changed since then. Today's viruses and worms are malign and aim for making profit. They attack now everything connected to a network: Windows PCs, but also Linux PCs and Macs; iPhones and other mobile devices; directly the operating system, but also applications like Adobe Reader (PDF), Firefox, ...

*Read the full article at: <http://cds.cern.ch/record/1324840?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1324840?ln=fr>*

Bye, Bye, Windows XP security... Welcome infections!

Rest in peace, Windows XP. Since your birth on 25 October 2001, you have struggled hard to survive this harsh Internet world. You fell prey to "Melissa", "Sasser" and "Conficker", and brought CERN its last large-scale infection with "Blaster" in 2004.

*Read the full article at: <http://cds.cern.ch/record/1694092?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1694092?ln=fr>*

Network Security

After Prism & Tempora: How much monitoring is OK for CERN?

Edward Snowden's revelations about the "Prism" and "Tempora" surveillance operations, run by the NSA in the US and GCHQ in the UK respectively, created quite a stir! Why has the witch hunt of a whistle-blower dominated newspaper headlines when there appears to have been no outcry over the fact that two countries have deeply penetrated our digital lives for so long?!

*Read the full article at: <http://cds.cern.ch/record/1566881?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1566881?ln=fr>*

The Lure of Wireless Encryption

Following our article entitled "Jekyll or Hyde? Better browse securely" in the last issue of the Bulletin, some people wondered why the CERN wireless network is not encrypted...

*Read the full article at: <http://cds.cern.ch/record/1551258?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1551258?ln=fr>*

Encryption is Useless!?

This week FTP (the file transfer protocol) celebrated its 40th birthday - and will hopefully retire soon! While a nice and simple means of transferring files, it is totally insecure: both the transferred contents and the authentication password are transferred unencrypted. FTP is not the only protocol that transfers data unencrypted: standard web traffic ("HTTP") and e-mail ("SMTP") are not encrypted either.

*Read the full article at: <http://cds.cern.ch/record/1345762?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1345762?ln=fr>*

Email & Web Security

Jekyll or Hyde? Better browse securely

Surfing the web is like walking through London in 1886. Usually you meet nice Dr Jekyll, interact with him and everything is fine. But at other times, at night, you might encounter the malicious Mr Hyde. He just wants your money and your secrets, and wants to take advantage of you.

*Read the full article at: <http://cds.cern.ch/record/1546809?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1546809?ln=fr>*

Browsing the Internet: good-bye anonymity!

Do you consider browsing the Internet to be your private business? When visiting random websites, how far do you assume you are anonymous? Would it matter to you that Google or Facebook can profile your browsing behaviour in order to better target you with advertisements? Did you notice that you already get targeted ads when you are logged on to Google or Facebook even if you are visiting completely different websites? If matters to you, note that browsing anonymously on the Internet is far from easy.

*Read the full article at: <http://cds.cern.ch/record/1450931?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1450931?ln=fr>*

Don't let your mail leak

At CERN, data privacy is of paramount importance, and we are currently developing a comprehensive data protection policy. For example, your CERN mailbox and your "private" folders on AFS and DFS are considered yours...

*Read the full article at: <http://cds.cern.ch/record/1442980?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1442980?ln=fr>*

Don't screw up your web

Publish or perish. Given the large variety of information which needs to be published, you have the freedom at CERN to deploy your own web-server and put your data online on the Internet. Web content management systems like Joomla! or WordPress together with dedicated add-ons and modules make it easy to quickly create a posh look-and-feel. But hold on. With this freedom also comes responsibility!

*Read the full article at: <http://cds.cern.ch/record/1431029?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1431029?ln=fr>*

You've received a Hallmark E-Card? Delete it!

Christmas is coming! Time to send to your loved ones a nice Christmas card, and maybe receive one too. But hold on... you've already received a Hallmark card by e-mail, or even two? Watch out.

*Read the full article at: <http://cds.cern.ch/record/1403040?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1403040?ln=fr>*

Cloud Security

Prison or “Prism”? Your data in custody

“Send your data into the cloud and make it... vaporize” was the title of one of our Bulletin articles in 2011. We were not precise enough. We should have entitled it “Send your data into the cloud and make it... available to a national security agency”.

*Read the full article at: <http://cds.cern.ch/record/1554961?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1554961?ln=fr>*

When the “Lion” eats your data

Welcome to “Mountain Lion” - Apple’s most recent operating system for Macs. More than 200 new and useful functions come with this version*. But hold on! New and useful? With this Lion comes the full integration into Apple’s “iCloud”, the same iCloud already used for iPhones and iPads.

*Read the full article at: <http://cds.cern.ch/record/1473672?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1473672?ln=fr>*

Send your data into the cloud and make it... vaporize

“Cloud computing” --- the term is as nebulous as real clouds.

*Read the full article at: <http://cds.cern.ch/record/1383877?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1383877?ln=fr>*

Mobile Security

Backed up and gone...

Remember how easy it is to lose your passwords for web applications (“Don’t let Chrome expose your passwords”)? This time we go bigger and discuss how easy it is to lose the passwords for every wireless access point you’ve visited. You just need to be running Android on your smartphone...

Read the full article at: <http://cds.cern.ch/record/1625989?ln=en>
L’article en français est également disponible : <http://cds.cern.ch/record/1625989?ln=fr>

BYOD: Bring your own disaster

Have you ever heard of “BYOD”? No, it is not a pop band. Try again. It is short for “Bring Your Own Device” (the French use “AVEC” - “Apporter Votre Equipement personnel de Communication”) and describes an option long since offered at CERN: the possibility to bring along your personal laptop, smartphone or PDA, use it on CERN premises and connect it to the CERN office network. But hold on. As practical as it is, there is also a dark side.

Read the full article at: <http://cds.cern.ch/record/1606798?ln=en>
L’article en français est également disponible : <http://cds.cern.ch/record/1606798?ln=fr>

Android is the new Windows

Do you recall the early virus attacks in the early 2000s? “Blaster”, “I love you” and “Slammer” were attacking the pretty much unprotected Microsoft Windows operating system.

Read the full article at: <http://cds.cern.ch/record/1542792?ln=en>
L’article en français est également disponible : <http://cds.cern.ch/record/1542792?ln=fr>

... and thank you for your mobile data!

Do you recall our Bulletin articles “Smartphone lost - Privacy gone” and “Your privacy is paramount”? In an interesting twist, we recently learned of a senior CERN staff member who returned his old smartphone to the CERN Telecom Service in exchange for a new phone. Guess what came with it? All his e-mails and plenty of personal data. Privacy, anyone?

Read the full article at: <http://cds.cern.ch/record/1490689?ln=en>
L’article en français est également disponible : <http://cds.cern.ch/record/1490689?ln=fr>

One photo to rule your phone

Have you ever seen those black-wide squares (picture below) called “Quick Response Codes”? Such QR tags are the two-dimensional forms of EAN codes (International Article Number, the black-white bars scanned at Migros’ check-outs) encoding a web address. Scanning those codes with your smart phone can lead you to a webpage, send an SMS or an e-mail depending on the contents of the tag. Beautiful, isn’t it? But wait. Can you trust that QR tag? What if the QR tag

leads to something malicious? Just to add more fun, we have recently heard about a vulnerability for Android devices prior to version 4.1.1 on its so-called “USSD code handling”.

Read the full article at: <http://cds.cern.ch/record/1482415?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1482415?ln=fr>

Smartphone lost - Privacy gone

Who doesn't own an iPhone, Android or Blackberry mobile phone today? Lucky you if you don't! In previous issues (Issue 06/07, 2012 and Issue 32/33/34, 2011) we have pointed out their lack of security. But what happens if you lose your smartphone or it gets stolen?

Read the full article at: <http://cds.cern.ch/record/1456530?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1456530?ln=fr>

Is your Android running a temperature?

You might have heard about Botnets, i.e. networks of infected (Windows) computers which are unwittingly under control by a malicious party. Public examples of botnets-in-action are attacks against the FBI, the U.S. Department of Justice, or against Universal and Warner Music as a retaliation for the shutdown of Megaupload.com. But have you ever heard of a Botnet made of Android phones?

Read the full article at: <http://cds.cern.ch/record/1421243?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1421243?ln=fr>

iphones, Androids, and history repeating

Remember when everyone was bashing Bill Gates because his operating system was insecure and a primary target for malicious software? While Microsoft has (tried to) improved on this, the IT world keeps on turning and the new target is your mobile phone. The Android and iPhone market is still growing. Can you live without your mobile phone today? Probably not. Mobile phones have become part of our identity.

Read the full article at: <http://cds.cern.ch/record/1372599?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1372599?ln=fr>

Passwords

No certificate, no chocolate

Are you already ready to use “certificates” to log into CERN or to connect to the global “eduroam” wireless network? No, I am not talking about your birth certificate, medical certificates or academic certificates. I am referring to “certificates” used for authentication where you would usually use a password.

Read the full article at: <http://cds.cern.ch/record/1633174?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1633174?ln=fr>

Don't let Chrome expose your passwords

Do you still struggle with remembering your password? Is this despite our many attempts to help you: “Train your Brain: Don't put your password on paper!” (article here), “Creativity@CERN” (article here) and “Maths to the rescue!” (article here)? Then you might have considered the “save your password” features in Chrome, Firefox or Internet Explorer... these features remember your Facebook, CERN, Twitter, Amazon and ebay passwords. But be careful: it might be easy for someone to read them!

Read the full article at: <http://cds.cern.ch/record/1624396?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1624396?ln=fr>

Maths to the rescue!

Do you recall our article on “Creativity@CERN” and the problem of creating good, memorable passwords? Given the feedback we've received, it still does not seem to be that easy.

Read the full article at: <http://cds.cern.ch/record/1561145?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1561145?ln=fr>

Creativity@CERN

Aren't we innovative and creative people? Building complex accelerators and doing sophisticated physics analysis is not easy and requires a lot of excellent brains. Some items of hardware are pure works of art, worthy of a place in an art museum. Some software takes advantage of all the finesse of computer science to optimize every last bit of computing power. So, yes. We are. Innovation and creativity are our middle names.

Read the full article at: <http://cds.cern.ch/record/1537306?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1537306?ln=fr>

Train your brain: Don't put your password on paper!

I completely acknowledge that constructing a good password can be difficult. And remembering it for some time isn't easy, either. However, noting it down on a sheet of paper and hiding it in a drawer in your office (or even attaching a sticky note to your monitor) isn't a valid solution. It violates CERN Computing Rules.

Read the full article at: <http://cds.cern.ch/record/1446268?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1446268?ln=fr>

1000 passwords exposed, what about yours?

In the last three issues of the Bulletin, we have stressed the importance of the secrecy of your password. Remember: Your password should be treated like a toothbrush: do not share it, and change it regularly! And this is not only valid for your CERN password, but also for any other password you use to log into your university or laboratory, Facebook or Twitter portals, or other web sites.

Read the full article at: <http://cds.cern.ch/record/1368912?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1368912?ln=fr>

Holidays Come - Passwords Go

The holiday season is approaching and with it, the best chance of losing your password!!

Read the full article at: <http://cds.cern.ch/record/1366034?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1366034?ln=fr>

What is a good Toothbrush, erm, Password?

Do you remember the answer to the question posed in the previous issue of the Bulletin? "Your password should be treated like a toothbrush: do not share it and change it regularly!" After our last article, we received a series of questions on how to choose a good password and remember it easily... Thus, here we go.

Read the full article at: <http://cds.cern.ch/record/1360262?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1360262?ln=fr>

What do passwords and toothbrushes have in common?

Your password is your entry token into the digital world. eBay, Amazon, Facebook, Twitter, FNAL, DESY, and CERN - all ask you for a password to authenticate and prove that you are you. And vice versa. If I know your password, I can impersonate you and use your money to buy from eBay or Amazon, post nasty messages on your Twitter or Facebook profile, or misuse CERN's/DESY's/FNAL's computing facilities in your name!

Read the full article at: <http://cds.cern.ch/record/1357349?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1357349?ln=fr>

When a person leaves - access rights remain!

We have been contacted recently by an embarrassed project manager who just figured out that a student who left at the end of 2013 still had access rights to read the whole project folder in February 2014: "How can that be?! In any other company, access rights would be purged at the same time as an employment contract terminates." Not so at CERN.

Read the full article at: <http://cds.cern.ch/record/1668622?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1668622?ln=fr>

Copyrights

Getting a better image from the Organization

Do you make regular presentations about CERN or CERN's activities to the public? Do you manage public webpages hosted by CERN? Do you edit or contribute to CERN publications? Besides plenty of text, every good presentation, webpage or publication is usually spruced up with visual content: graphics, photos or even videos. But have you ever thought about whether you actually have the proper rights to use such imagery?

Read the full article at: <http://cds.cern.ch/record/1645412?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1645412?ln=fr>

Bad (Re)Presentations

This time, we would like to address copyright violations (again) - but with a twist. While previous articles focussed on "Music, videos and the risk for CERN" or on software licences, the focus is now on using photos, music and images "found" on the Web for presentations, publications and web pages...

Read the full article at: <http://cds.cern.ch/record/1544570?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1544570?ln=fr>

Software licenses: Stay honest!

Do you recall our article about copyright violation in the last issue of the CERN Bulletin, "Music, videos and the risk for CERN"? Now let's be more precise. "Violating copyright" not only means the illegal download of music and videos, it also applies to software packages and applications.

Read the full article at: <http://cds.cern.ch/record/1471401?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1471401?ln=fr>

Music, videos and the risk for CERN

Do you like listening to music while you work? What about watching videos during your leisure time? Sure this is fun. Having your colleagues participate in this is even more fun. However, this fun is usually not free. There are artists and the music and film companies who earn their living from music and videos.

Read the full article at: <http://cds.cern.ch/record/1462284?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1462284?ln=fr>

Data Protection

How private is “private”?

What a surprise it would be for you to discover that everyone at CERN can access your Windows “My Documents” folder or your AFS home-folder? Reading your private letters? Looking at your private photos? Digging through your confidential documents? Would you be embarrassed? You would not be the first.

*Read the full article at: <http://cds.cern.ch/record/1647826?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1647826?ln=fr>*

Let's play hide and seek!

This week, we would like you to play a small online game called “Virtual Hide & Seek”. The rules are simple: some of our colleagues have published some sensitive or confidential documents on CERN's central services like Indico, CDS, EDMS or TWiki, as well as on our many websites. Your mission, should you choose to accept it: find them!

*Read the full article at: <http://cds.cern.ch/record/1493451?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1493451?ln=fr>*

Your privacy is paramount!

May I read your e-mails or join you while you browse the web? What if I access all your personal documents on the DFS or AFS disk spaces? I guess you have nothing to hide and all that information is related to your professional duties... so why would you care?

*Read the full article at: <http://cds.cern.ch/record/1478918?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1478918?ln=fr>*

“Clas-si-fied (/ˈklæsɪfaɪd/)” - What's that?

Have you ever thought about what information at CERN should or must be classified as confidential? Or public? What does “confidential” mean anyway? European law, for example, requires proper protection of your medical files. At CERN, for security reasons your passwords are yours and only yours (remember: “Your password is your toothbrush”). And it is in your own interest that your credit card details are kept confidential, too. But what about your office location, your CERN phone number, or your official photo for your CERN card?

*Read the full article at: <http://cds.cern.ch/record/1453808?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1453808?ln=fr>*

Data Protection for All

What a stir... was caused by two articles in the last issue of the Bulletin, on “New Snail Mail Scanning Service” and “CERN meets Facebook”!

*Read the full article at: <http://cds.cern.ch/record/1434741?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1434741?ln=fr>*

How to get properly rid of confidential data?

Have you ever bought a used laptop on ebay? Try it and you might not only get (hopefully) functional hardware, but also a bunch of personal files, intriguing photos, sensitive documents, etc. Not everybody worries enough to clean the local hard disks properly before selling their equipment or giving it away. So the next owner of the hard disk can comfortably crawl through the remaining data, and use it at his or her convenience...

*Read the full article at: <http://cds.cern.ch/record/1428518?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1428518?ln=fr>*

Classified

In the last issue of the Bulletin, we have discussed recent implications for privacy on the Internet. But privacy of personal data is just one facet of data protection. Confidentiality is another one. However, confidentiality and data protection are often perceived as not relevant in the academic environment of CERN.

*Read the full article at: <http://cds.cern.ch/record/1352172?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1352172?ln=fr>*

Privacy, who cares?

In mid-April, the Sony “Playstation” and “Online Entertainment” networks were compromised and the records of nearly 100 million(!) users (names, addresses, dates of birth, e-mail addresses) were stolen. It even seems that the credit card numbers of these users were lost, too.

*Read the full article at: <http://cds.cern.ch/record/1349244?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1349244?ln=fr>*

Coming soon, a pragmatic Data Protection Policy for an open Organisation

Like any other organisation/employer, CERN holds confidential data, e.g. medical records, personnel files, files on harassment cases, NDAs & contracts, credit card information, and even unpublished scientific results. Unfortunately, our current methods of handling such documents are inadequate owing to a lack of clarity with regard to responsibilities and obligations.

*Read the full article at: <http://cds.cern.ch/record/1665387?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1665387?ln=fr>*

Easy encryption for CERN laptops

The number of laptops stolen from or lost by CERN staff and users is not negligible. On average, four to five devices are reported lost or stolen to the CERN Fire Brigade every month.

*Read the full article at: <http://cds.cern.ch/record/1665388?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1665388?ln=fr>*

Policies

CERN: Digitally open, too

The Open Days are here!! From tomorrow onwards, we will be welcoming thousands of people to CERN. No barriers, no boundaries!

*Read the full article at: <http://cds.cern.ch/record/1601976?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1601976?ln=fr>*

Don't tempt me!

Over your CERN career, have you ever changed activities, functions or responsibilities, but nevertheless kept the access to your “old” control systems or computing services? Accessing the systems for which you are no longer responsible seems innocent enough, because you just want to help by using your previous work and experience but... Does this sound familiar to you? Let's think this one through because it may have bad consequences.

*Read the full article at: <http://cds.cern.ch/record/1599503?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1599503?ln=fr>*

The Naked Blunder

In the past, we have published many different articles on a multitude of aspects of computer security and on the risk to CERN and to you when you use your computer at CERN or at home. Some were relevant to all of us, others only to a minority. This time, we would like to raise a rather delicate and fortunately rare issue: the consultation of pornographic websites and why it is forbidden at CERN.

*Read the full article at: <http://cds.cern.ch/record/1562581?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1562581?ln=fr>*

Why “Security” is not ME...

Thank you all for your feedback on our latest Bulletin article on “Security is YOU!”. Indeed, I can confirm that at CERN you are, in the first instance, responsible for: the computer security of the laptops, smart phones and PCs you use; the computing accounts and passwords you own; the files and documents you hold; the programs and applications you have installed or, in particular, written; and the computer services and systems you manage. In the free and liberal academic environment of CERN, I, as Computer Security Officer, decline that general responsibility.

*Read the full article at: <http://cds.cern.ch/record/1498682?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1498682?ln=fr>*

“Security” is YOU!

Usually, people consider “Computer Security” a technical problem: firewalls, intrusion detection, anti-virus software, encryption... but I don't. I consider “Computer Security” being like swimming or crossing a road.

Read the full article at: <http://cds.cern.ch/record/1496408?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1496408?ln=fr>

Social Media - Dos and Don'ts

Do you blog frequently? Send tweets about what you've done? Keep a lively Facebook profile?
Comment regularly on interactive forums? Many of us do.

Read the full article at: <http://cds.cern.ch/record/1670290?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1670290?ln=fr>

Secure Coding

Stop fighting alone, let synergy rule!

Could it be true, as it seems to me, that CERN still has manpower to spare? I thought that now, during LS1, resources were scarce and everybody was very busy. But apparently not. We are getting more requests than ever to open firewalls for stand-alone web servers running local databases and custom web applications.

*Read the full article at: <http://cds.cern.ch/record/1567097?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1567097?ln=fr>*

Why can't I sue my software provider?

Imagine buying a new car, fixing its number plates on and driving it off to the autobahn in order to test whether the 250km/h top speed on the speed meter is genuine. However, there's too much traffic, and you have to slow down. You hit the brakes but they don't respond. You break through the crash barrier, enter a field and manage to stop the car. You are not hurt, but the car is a write-off...

*Read the full article at: <http://cds.cern.ch/record/1554541?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1554541?ln=fr>*

A Short Tale of the Black Sheep of -ITY

Once upon a time, computer engineers of the ancient world used the abbreviation of “-ITY” ([eye-tee]) as a shorthand for “Information TechnologY”. It was an appropriate abbreviation as it reminded everyone of the core purposes and aspects of information technology, which made not only the computer engineers, but also their clients, happy.

*Read the full article at: <http://cds.cern.ch/record/1504850?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1504850?ln=fr>*

Raise your defence: a baseline for security

It is an unfair imbalance: the (computer) security of a system/service is only as strong as the weakest link in the chain of protection. This provides attackers with an incredible advantage: they can choose when to attack, where and with which means. The defence side is permanently under pressure: they must defend at all times all assets against all eventualities. For computer security, this means that every computer system, every account, every web site and every service must be properly protected --- always.

*Read the full article at: <http://cds.cern.ch/record/1398660?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1398660?ln=fr>*

An example of flawed code

Do you recall our small exercise in the last issue of the Bulletin?

*Read the full article at: <http://cds.cern.ch/record/1379547?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1379547?ln=fr>*

Do you write secure code?

At CERN, we are excellent at producing software, such as complex analysis jobs, sophisticated control programs, extensive monitoring tools, interactive web applications, etc. This software is usually highly functional, and fulfils the needs and requirements as defined by its author. However, due to time constraints or unintentional ignorance, security aspects are often neglected. Subsequently, it was even more embarrassing for the author to find out that his code flawed and was used to break into CERN computers, web pages or to steal data...

*Read the full article at: <http://cds.cern.ch/record/1376430?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1376430?ln=fr>*

Improve software, avoid blunder

Recently, a severe vulnerability has been made public about how Apple devices are wrongly handling encryption. This vulnerability rendered SSL/TLS protection useless, and permitted attackers checking out a wireless network to capture or modify data in encrypted sessions.

*Read the full article at: <http://cds.cern.ch/record/1698263?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1698263?ln=fr>*

Risk Management

Cyber-Attacks and the Risks for CERN

In the previous Bulletin, we discussed the cyber-risks for the accelerator complex. However, looking at the broader picture, the cyber-risks for CERN are much more diverse.

*Read the full article at: <http://cds.cern.ch/record/1520152?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1520152?ln=fr>*

Hacking control systems, switching... accelerators off?

In response to our article in the last Bulletin, we received the following comment: "Wasn't Stuxnet designed to stop the Iranian nuclear programme? Why then all this noise with regard to CERN accelerators? Don't you realize that 'computer security' is not the raison d'être of CERN?". Thank you for this golden opportunity to delve into this issue.

*Read the full article at: <http://cds.cern.ch/record/1514590?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1514590?ln=fr>*

Hacking control systems, switching lights off!

Have you ever heard about "Stuxnet"? "Stuxnet" was a very sophisticated cyber-attack against the Iranian nuclear programme. Like in a spy movie, the attackers infiltrated the uranium enrichment plant at Natanz, arranged for infected USB sticks to be inserted into local PCs, and then the USB viruses did the rest.

*Read the full article at: <http://cds.cern.ch/record/1510561?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1510561?ln=fr>*

Miscellaneous

Security bingo for administrators

Have you ever thought about the security of your service(s) or system(s)? Show us and win one of three marvellous books on computer security! Just print out this page, mark which of the 25 good practices below you already follow, and send the sheet back to us at Computer.Security@cern.ch or P.O. Box G19710, by November 14th 2011.

*Read the full article at: <http://cds.cern.ch/record/1394611?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1394611?ln=fr>*

Security bingo for the paranoid

We have received complaints that the previous SECURITY BINGO was too easy... So, are you extremely cautious of computer security? Show us and win one of three marvellous books on computer security! Just print out this page, mark which of the 25 good practices below you already follow, and send the sheet back to us at Computer.Security@cern.ch or P.O. Box G19710, by October 31st 2011.

*Read the full article at: <http://cds.cern.ch/record/1391753?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1391753?ln=fr>*

Security Bingo

Want to check your security awareness and win one of three marvellous books on computer security? Just print out this page, mark which of the 25 good practices below you already follow, and send the sheet back to us by 31 October 2011 at either Computer.Security@cern.ch or P.O. Box G19710.

*Read the full article at: <http://cds.cern.ch/record/1387913?ln=en>
L'article en français est également disponible : <http://cds.cern.ch/record/1387913?ln=fr>*

