2-FACTOR AUTHENTICATION TOWN HALL

DECEMBER 17, 2015
AGENDA

Randy Marchany
Scott Midkiff
Questions
2-factor enrollment opportunity
You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.security.vt.edu/ouch

Username & Passwords
Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:
- Your bank or financial accounts, where they can steal or transfer your money.
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.
- Your UPS or Fedex accounts, where they ship stolen goods in your name.

Email Harvesting
Once hacked, cyber criminals can read your email for information they can sell to others, such as:
- All the names, email addresses and phone numbers from your contact list.
- All of your personal or work email.

Virtual Goods
Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:
- Your online gaming characters, gaming goods or gaming currencies.
- Any software licenses, operating system license keys, or gaming licenses.

Botnet
Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:
- Sending out spam to millions of people.
- Launching Denial of Service attacks.

Identity Hijacking
Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:
- Your Facebook, Twitter or LinkedIn account.
- Your email accounts.
- Your Skype or other IM accounts.

Web Server
Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:
- Hosting phishing websites to steal other people’s usernames and passwords.
- Hosting attacking tools that will hack people’s computers.
- Distributing child pornogrophy, pirated videos or stolen music.

Financial
Once hacked, cyber criminals can scan your system looking for valuable information, such as:
- Your credit card information.
- Your tax records and past filings.
- Your financial investments and retirement plans.

Extortion
Once hacked, cyber criminals can take over your computer and demand money. They do this by:
- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.
- Encrypting all the data on your computer and demanding payment to decrypt it.
- Tracking all websites you visit and threatening to publish them.

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com
Login to Scholar Course Management System

If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your Guest Account.

Username
Password

Forgot username or password?

Warn before logging into other sites.

Login  Clear

Switch to high security PDC login.

Security Notice

For security reasons, please close your web browser when you have finished accessing services that require authentication.
Virginia Tech Central Authentication Service - Google Chrome

Login to Scholar Course Management System
If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your Guest Account.

Username
Password

Forgot username or password?

Login  Clear

Switch to high security PDC login.

Security Notice
For security reasons, please close your web browser when you have finished accessing services that require authentication.

© 2008-2014 Virginia Polytechnic Institute and State University.
The VT CAS logo is a derivative of NIST Logo by nist.gov, licensed under BY-NC-SA.
How passwords are discovered...

Attacks use a variety of password discovery techniques, including the use of powerful tools that are freely available on the Internet.

- **Social Engineering**: Attackers use social engineering skills to coerce users into revealing their passwords.
- **Manual Guessing**: Attackers use personal information "cribs" (such as name, date of birth, etc.) to guess common passwords.
- **Interception**: Passwords can be intercepted as they are transmitted over a network.
- **Stealing Passwords**: Attackers can steal passwords that have been stored insecurely. This can include handwritten passwords hidden close to a device.
- **Shoulder Surfing**: Observing someone typing in their password.
- **Key Logging**: An installed keylogger intercepts passwords when they are typed into a device.
- **Brute Force**: Automated guessing of billions of passwords until the correct one is found.
- **Searching**: Searching IT infrastructure for electronically stored password information.

...and how to improve your system security.

The following advice will reduce the workload on your users, making your system more secure as a result.

Help users generate appropriate passwords:
- Put technical defences in place so that simpler passwords can be used.
- Steer users away from choosing predictable passwords, and prohibit the most common ones.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Help users cope with "password overload":
- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication or suspicion of compromise.
- Allow users to reset passwords easily, quickly and cheaply.
PHISHING
Be aware of unexpected email, messages, and attachments.

No legitimate business will ever ask for your credentials by email!
ONE USER’S EXPERIENCE

User account identified as compromised

- 4HELP contacted her to change her passwords

Working from home in the evening on personal PC

User changed password second time from work desktop

User received email of Direct Deposit change

As a precaution user changed password from “clean” machine

- During the process user gets call on personal cell phone

User had passwords saved in browser!

Account Recovery Options

www.security.vt.edu