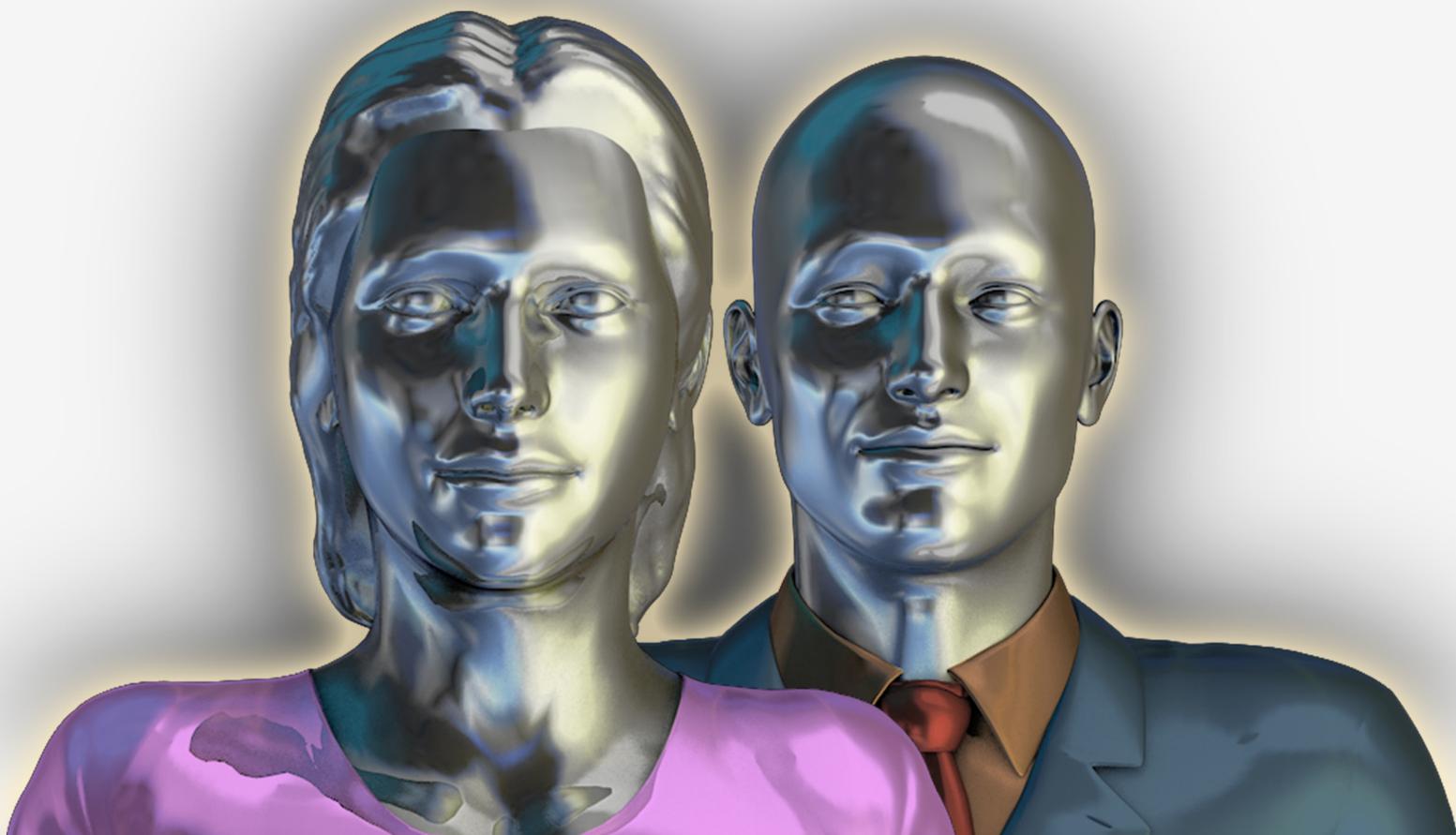


# You Are the Target

Many people mistakenly believe that their computer or information has no value and cyber attackers would never target them. In reality, individuals like you are a target. You and your computer are under attack almost every day. The first step to protecting yourself is realizing you are a target.



This newsletter is published by Villanova University's security team.  
For more information, please contact us at:

[support@villanova.edu](mailto:support@villanova.edu)

**THE INNOVATIVE**  
S TECHNOLOGY SOLUTIONS & SERVICES

# You Are the Target

One of the most important things for you to understand is that you are a target. Many people mistakenly believe that cyber attackers only target our databases or web servers. In reality, they also target individuals like you. While these attackers use a variety of sophisticated tools, they have learned that the simplest way to hack into an organization like ours is to target people like you. Let's take a look at how a group of cyber attackers might hack into our organization. While the following story did not happen, it illustrates common methods used to hack into an organization like ours.

Several months ago, a team of cyber attackers decided to target our organization. We are not sure what their motivation was. Perhaps they wanted to steal our sensitive information, make a political statement or gain access to one of our partners. All we know is that they began searching our website several weeks ago, learning everything they could about us. This included who we are, how we operate and the identities of our employees and staff. They then began to harvest employees' personal information from websites such as Facebook, YouTube, LinkedIn, Instagram and public forums.

Unfortunately, several employees had posted too much information about themselves and our organization. As a result, the attackers were able to build a complete picture of our organization and learn details about key members of our staff. Armed with this information, they launched their attack. Seven employees at our organization received emails that appeared to come from a package delivery service we commonly use. While these emails appeared to be legitimate, they were actually phishing emails created by the attackers. Each message contained an infected email attachment designed to bypass our anti-virus software and silently infect our computers.

Unfortunately, two of the targeted employees fell victim to the phishing emails by opening the attachments. Since their computers were not patched, they were quickly infected, giving the cyber attackers complete control. The attackers then installed keylogging software on the computers, enabling them to capture all of the employees' keystrokes. On one of the hacked computers, an employee was using a login and password they had shared with their coworkers. The attackers quickly harvested this information and were able to log into other systems throughout our organization. Because the attackers were using stolen, legitimate passwords, our security team did not detect them.

Over the next seven days, the attackers scanned the hard drives of numerous compromised systems, stealing every document, spreadsheet and presentation they could find. They soon transferred over 150 Gigabytes of confidential information out of our organization, including a key project we had been working on for over three months. Fortunately, an alert employee noticed several suspicious programs running on their computer and reported it. As a result, the attackers were finally detected and blocked from causing any more harm.

# You Are the Target

While this story is only an example, it demonstrates why we have security policies and controls. They are carefully designed to protect you and our organization, while also ensuring that we are compliant with important standards and regulations. This is why it is so important that you understand and follow our security policies.

You may not realize it, but you are also under attack when you and your family connect to the Internet at home. To help protect yourself, your family and our organization, always remember some core principles:

- Always be cautious and assume you are a target. You may not think you or your information has value, but it does.
- Attacks are a constant threat on the Internet. If something seems suspicious or too good to be true, it most likely is.



## Cyber Crime Is Highly Organized

Cyber criminals have become more and more sophisticated over the past decade. When cyber criminals first appeared, they often worked alone. They built their own attack tools, manually searched for and hacked into computers, stole people's account information and transferred stolen money or information by themselves. Today's cyber criminals are far more sophisticated. Each criminal now has their own specific field of expertise. By working together, they have developed their own highly organized community. For example, one group will specialize in developing and supporting sophisticated attack tools while another group will specialize in hacking other computers or laundering stolen money. An entire cybercrime economy has emerged, which is constantly improving its tactics and becoming more effective and efficient in making money. These criminals form a highly sophisticated threat, one that will be with us for many years to come.

This newsletter is published by Villanova University's security team.  
For more information, please contact us at:

[support@villanova.edu](mailto:support@villanova.edu)

**THE INNOVATIVE**  
TECHNOLOGY SOLUTIONS & SERVICES